Council of the European Union
General Secretariat

Interinstitutional files:
2025/0360 (COD)

Brussels, 04 June 2026

WK 7876/2026 INIT

LIMITE

SIMPL
ANTICI
DATAPROTECT
CYBER
TELECOM
CODEC
PROCIV
COMPET
MI

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Antici Group (Simplification)
Subject:	Omnibus VII (Digital): Written comments/suggestions from Member States on Presidency revised compromise text (P2B, GDPR, e-privacy/cookies, cyber)

Delegations will find attached the comments on the Presidency revised compromise text (deadline 02 June 2026) from the following Member States: AT, BE, CZ, DK, EE, ES, FI, FR, HR, HU, IT, LU, LV, MT, NL, PL, RO, SI, SE and SK.

Comments on the Presidency revised compromise text (P2B, GDPR, e-privacy/cookies, cyber) Deadline: ***2 June 2026***
From: NL, LU, IT, HR, FR, EE, DK, AT, MT, LV, HU, FI, CZ, BE, SK, SI, SE, RO, PL, ES **Updated: 04/06/2026 10:06**

Guidelines to be followed

Please kindly provide your contributions in the table below.

Drafting suggestions: you may use '**track changes**'* or formatting (for example **bold-underline** for additions and ~~strike-through~~ for deletions, **where necessary, in a different colour**). *Track changes can only be connected once the cursor is placed in editable areas (Drafting or Comments columns).

To make it feasible to consolidate all contributions, the structure of the table must not be changed, so **no rows can be added or deleted.**

New provisions may only be added in any of the **'existing cells'.**

Name of document: please add the **two initials** of your delegation's country followed by a space (to the MS Word document name), followed by any optional text, for example, for Austria: **AT comments on … .docx**

Thank you for your cooperation!

Commission proposal	Drafting suggestions and Comments
General Comments	LU (Drafting suggestions): On the cyber-related provisions, Luxembourg would like to thank the Presidency for the revised text, which we can support in its current form. On the national entry point, Luxembourg endorses the Presidency's approach and appreciates the consideration given to existing national structures, a crucial element in our assessment. Regarding the Estonian non-paper, Luxembourg acknowledges the potential added value of the proposal for Member States without national reporting solutions. However, adopting the open-source option would likely require Member States that already operate national notification systems to redevelop functionalities that are fully established and functioning at national level. This would create additional administrative and technical burdens without clear added benefit in our case.

Commission proposal	Drafting suggestions and Comments
	• Luxembourg is therefore not in a position to express specific support at this stage and considers it essential that the use of a potential open-source solution remains voluntary. IT (Comments): This submission has been jointly developed with France and the Netherlands as a common approach. EE (Comments): Estonia would like to thank the Presidency for the work done as well as for the opportunity to present written comments and considering our drafting suggestions. DK (Comments): DK general comment: None of the proposed changes since the Commission's original proposal are individually a red line for Denmark. However, we are concerned that the total amount of changes effectively means that there is not much simplification left and that we therefore are not living up to the political mandate, which was reflected in the original proposal from the Commission. For example, it is difficult to see any real simplification in the area of artificial intelligence, given the proposed amendments to the provision on the processing of special categories of data in that regard (Article 9(2)(k) and (5)), and the removal of Article 88c. The same applies in relation to the

Commission proposal	Drafting suggestions and Comments
	added requirements to the provision on processing of biometric data that is necessary for the purpose of confirming the identity of a data subject (Article 9(2)(l) and other provisions (removing disclosure from the proposed Article 13(5) etc.). We would therefore like to see a discussion on whether the proposal as a whole delivers on the mandate of simplification, as we find it increasingly hard to support the current direction. Similarly, we would like to see a discussion on the issue of the definition of personal data. Although we believe that guidance from the EDPB is better than nothing, we still see greater potential in writing the definition in the operative text. We do not think there has been sufficient discussion on which way to go on this issue. FI (Comments): FI thanks the Presidency for advancing the negotiations and the opportunity to submit detailed comments in writing. FI remains open for discussing the below points in further detail and advancing a balanced outcome. SK (Comments): **All SK comments are considered a preliminary position.** SI (Comments): In general, we support the direction of the compromise text put forward by the Presidency. However, we are of the opinión that the text would Benefit from further clarifications, both in the recitals and, where appropriate, in the operative provisions of the text. PL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): **If our proposals regarding the provisions are accepted, the wording of the recitals should be redrafted accordingly.** ES (Comments): **Spain.** As to the part concerning incident notifications, Spain considers that the current formulation strikes the right balance, responds to the concerns raised by Member States since the early stages of the negotiation and provides a workable basis for a Council mandate. A more prescriptive definition of the national entry point (whether through an enumerated task list or through a reformulation that implies a single technical interface) would reduce the flexibility that the text currently affords and risk excluding national architectures that are fully consistent with the objectives of the provision.
2025/0360 (COD)	DK (Comments): DK generally on GDPR: In addition, Denmark agrees with Spain and other Member States that the issue of automatic exchange of tax information with third countries should be discussed and eventually clarified as part of the omnibus proposal
Proposal for a	DK (Comments): DK on SEP: As stated repeatedly, Denmark would have preferred a stronger simplification mandate in the Council General approach. Denmark has benefited greatly from having one national reporting platform for reports based on the legislations mentioned in this omnibus. We maintain that a similar solution at EU-level would be beneficial. However, as there is no support for this amongst other Member States, we find that the comprise text

Commission proposal	Drafting suggestions and Comments
	does not impede our national solution, and thus we have few comments on how to further improve the text.
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	BE (Comments): BE also supports Spain's proposal on article 49
amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)	AT (Comments): At the outset, AT would like to express its support for the submission made by IT regarding the provisions Art 11, Art 23b and Recital (50a). This does, however, not prejudice the comments and statements contained in this document regarding the cyber aspects of the digital omnibus proposal. LV (Drafting suggestions): "Proposal for a REGULATION [..] amending Regulations [..] (EU) 2022/2554". LV (Comments): The reference to DORA (Regulation (EU) 2022/2554) should be reinserted in the title, as previously drafted: "Proposal for a REGULATION [..] amending Regulations [..] (EU) 2022/2554".

Commission proposal	Drafting suggestions and Comments
THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 and 114 thereof,	
Having regard to the proposal from the European Commission,	
After transmission of the draft legislative act to the national parliaments,	
Having regard to the opinion of the European Economic and Social Committee[1], 1 OJ C […], […], p. […].	
Having regard to the opinion of the European Central Bank[2], 2 OJ C […], […], p. […].	
Having regard to the opinion of the Committee of the Regions[3], 3 OJ C […], […], p. […].	
Acting in accordance with the ordinary legislative procedure,	
Whereas:	
(1) In its Communication on a simpler and faster Europe[4] , the Commission announced its commitment to an ambitious programme to promote forward-looking, innovative policies that strengthen the Union's competitiveness and radically lighten the regulatory load for people, businesses and administrations, while maintaining the highest standard in promoting the Union's values. Consequently, the Commission prioritised the	

Commission proposal	Drafting suggestions and Comments
proposal of immediate adjustments to legislation, including digital legislation, to address the competitiveness challenge of the Union. 4 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A simpler and faster Europe: Communication on implementation and simplification, COM(2025)47 final, 11 February 2025	
(2) Union digital legislation sets high standard in the Union and can be a powerful source of competitive advantage for businesses that abide by the rules, showing a world-leading mark of quality, safety and trustworthiness. Digital regulations have framed the clear rules of the game in the Union for responsible businesses, ensuring fairness and transparency in business-to-business relations, stimulating innovative business models, setting high standard of consumer protection and safety, and for the protection fundamental rights, not least privacy and data protection.	
(3) Union digital legislation has evolved incrementally over the past years, in response to the rapidly growing footprint of digital technologies in the Union's economy and societal dynamic, and in view of addressing emerging challenges and promoting business opportunities in the EU. Notwithstanding the Commission's commitment to a systematic 'stress test' of the digital rules, along with other Union rules, which might lead to further regulatory adjustments notably following the forthcoming Digital Fitness Check, as well as other targeted evaluations of digital rules, immediate regulatory changes are necessary. Consequently, this Regulation proposes a first set of amendments to the digital legislative framework, aimed at providing immediate regulatory clarifications that stimulate innovation in the Union market, and that cut administrative compliance costs in particular for businesses, while also streamlining supervisory and administrative costs for	

Commission proposal	Drafting suggestions and Comments
supervisory authorities and advisory bodies. The amendments also seek to provide clarity to individuals.	
(…)	
(27) This Regulation proposes a series of targeted amendments to Regulation (EU) 2016/679 for clarification and simplification, whilst preserving the same level of data protection. ~~Article 4 of Regulation (EU) 2016/679 provides that personal data is any information relating to an identified or identifiable natural person. In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. Taking into account the case-law of the Court of Justice of the European Union concerning the definition of personal data, it is necessary to provide further clarity on when a natural person should be considered to be identifiable. The existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person or entity, personal data for the purposes of the application of Regulation (EU) 2016/679. In particular, it should be clarified that information is not to be considered personal data for a given entity where that entity does not have means reasonably likely to be used to identify the natural person to whom the information relates. A potential subsequent transmission of that information to third parties who have means reasonably allowing them to identify the natural person to whom the information relates, such as cross-checking with other data at their disposal, renders that information personal data only for those third parties who have such means at their disposal. An entity for which the information is not personal data, in principle, does not fall within the scope of application of Regulation (EU) 2016/679. In this respect the Court of Justice of the European Union has held that a means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data~~	EE (Comments): Estonia supports the amendments. AT (Comments): AT **continues to support** that the current definition of 'personal data' remains unchanged. MT (Comments): We strongly support the proposed deletions. FI (Comments): FI can support this recital text. SE (Drafting suggestions): Regarding pseudonymised data, the existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person, personal data. Pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable.

Commission proposal	Drafting suggestions and Comments
~~subject is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and labour. An example of a prohibition against reidentification can be found in the obligations of health data users in Article 61(3) of Regulation (EU) 2025/327 of the European Parliament and of the Council[5]. The Commission, together with the European Data Protection Board, should support controllers in the application of this updated definition by stipulating technical criteria in an implementing act.~~ 5 ~~Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj)~~	Data which are in themselves impersonal may become 'personal' in nature where they are put at the disposal of other persons who have means reasonably likely to enable the data subject to be identified. In so far as it cannot be ruled out that those third parties have means reasonably allowing them to attribute pseudonymised data to the data subject, such as cross-checking with other data at their disposal, the data subject must be regarded as identifiable as regards both that transfer and any subsequent processing of those data by those other persons. A means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and labour. Means reasonably likely to be used by an entity to identify a natural person directly or indirectly include inter alia legal means of obtaining additional information from another person making it possible to identify the data subject as well as the singling out and cross-checking with other data at their disposal.
(27a) In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. The identification of a natural person should be assessed by the controller or the processor, considering the actual technical, organisational and legal capabilities of the controller or processor. In light of the interpretation provided in the case-law of the Court of Justice of the European Union, it is important to provide further clarity on when a natural person should be considered to be identifiable following the application of pseudonymisation to personal data and the transmission to a recipient. The European Data Protection Board should ensure consistency and support controllers by adopting an opinion on pseudonymisation and anonymisation, assessing and specifying the state of the art of available techniques, as well as the	NL (Drafting suggestions): (27a) In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. The identification of a natural person should be assessed by the controller or the processor, considering the actual technical, organisational and legal capabilities of the controller or processor. In light of the interpretation provided in the case-law of the Court of Justice of the European Union, it is important to provide further clarity on when a natural person should be considered to be identifiable following the application of pseudonymisation **and anonymisation** to personal data and the transmission to a recipient. The European Data Protection Board should

Commission proposal	Drafting suggestions and Comments
technical and organisational measures and criteria to apply pseudonymisation and anonymisation to personal data effectively and by clarifying circumstances whether and when the application of pseudonymisation to personal data may effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable. The opinion should also address the processing to be undertaken and other measures to be applied in order to effectively render personal data anonymous. It is important that the Board carries out a public consultation with relevant stakeholders prior to issuing its opinion. While controllers remain fully responsible to determine and demonstrate whether pseudonymised data do not lead to re-identification of data subjects by persons other than the controller, the opinion should support and provide guidance to controllers regarding the effective application of pseudonymisation to personal data.	ensure consistency and support controllers **and processors** by adopting an opinion on pseudonymisation and anonymisation, assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to apply pseudonymisation and anonymisation to personal data effectively and by clarifying circumstances whether and when the application of pseudonymisation to personal data may effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable. The opinion should also address the processing to be undertaken and other measures to be applied in order to effectively render personal data anonymous. It is important that the Board carries out a public consultation with relevant stakeholders prior to issuing its opinion. While controllers remain fully responsible to determine and demonstrate whether pseudonymised data do not lead to re-identification of data subjects by persons other than the controller, the opinion should support and provide guidance to controllers regarding the effective application of pseudonymisation to personal data. NL (Comments): NL proposes some editorial changes to further improve the consistency of recital 27a and Article 29a. IT (Drafting suggestions): ***(27a) In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. The identification of a natural person should be assessed ex ante and in concreto, considering the actual technical, organisational and legal capabilities of the controller. Taking into account the case-law of the Court of Justice of the European Union, it is important to provide further clarity on when a natural person***

Commission proposal	Drafting suggestions and Comments
	should be considered to be identifiable following the application of pseudonymisation to personal data and the transmission to a recipient. ~~***The European Data Protection Board should ensure consistency and support controllers by adopting an opinion on pseudonymisation and anonymisation, assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to apply pseudonymisation to personal data effectively, and clarifying circumstances whether the application of pseudonymisation to personal data may effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable. It is important that the Board carries out a public consultation with relevant stakeholders prior to issuing its opinion. While controllers remain fully responsible to determine and demonstrate whether pseudonymised data do not lead to re-identification of data subjects by persons other than the controller, the opinion should support and provide guidance to controllers regarding the effective application of pseudonymisation to personal data.***~~ IT (Comments): The proposed amendment should be supported because: • It clarifies that the data controller's ability to identify the data subject must be reasonable and not absolute. This avoids interpretations of the GDPR that impose disproportionate and costly obligations; • It clarifies that if pseudonymization does not allow the recipient of the data to re-identify the data subject, the data are effectively anonymous for the recipient. This is crucial for medical and scientific research because it simplifies, for example, the exchange of clinical data. A hospital can contribute to research by providing pseudonymized patient data to research institutions, which can treat it as anonymous because they have no way of identifying the patients.

Commission proposal	Drafting suggestions and Comments
	Without these paragraphs, confusion will continue regarding how to apply the GDPR to both information society services and medical and scientific research, generating inertia without any real benefit for citizens. However, the reference to the role of the EDPB should be removed, as it risks reintroducing organizational, bureaucratic, and technical burdens, and moreover, within a timeframe incompatible with the needs of research institutions and businesses. We propose deleting the following sentences (see second column): This would allow individual national data protection authorities to assess ex post whether the decisions of individual data controllers are legally correct. This would reinforce the principle of accountability enshrined in the GDPR, which leaves data controllers legally responsible for their decisions, rather than imposing preventive and general requirements that, as such, are insufficiently flexible. FR (Comments): **Les autorités françaises peuvent soutenir les amendements apportés aux considérants 27a et 27b pour appuyer l'implication nécessaire du CEPD au soutien des responsables de traitements et des sous-traitants en matière de pseudonymisation effective. Les acteurs ont en effet besoin d'être accompagnés par une doctrine concrète, opérationnelle, effective et nourrie des retours des acteurs au travers de consultations préalables pour lui permettre de saisir les enjeux concrets du terrain. Elles regrettent néanmoins la suppression de la précision suivant laquelle le caractère identifiant doit être évalué ex ante et in concreto, qui figurait dans la précédente version du considérant 27a.** EE (Comments): Estonia supports the amendment.

Commission proposal	Drafting suggestions and Comments
	AT (Comments): AT **continues to support** assigning the competence to issue guidelines regarding pseudonymisation and identifiability of natural persons to the EDPB. AT **continues to support** the proposed Recital 27a. MT (Comments): We maintain our reservations regarding the reference to the issuance of an opinion by the EDPB in accordance with Article 64(2) GDPR. According to Article 64(2) GDPR, only supervisory authorities, the Chair of the Board or the Commission may request that any matter of general application be examined by the Board with a view to obtaining an opinion. Thus, Article 64(2) GDPR provides for a discretionary possibility to request an Opinion, whilst the current drafting appears to introduce a more systematic or prescriptive trigger by requiring the Chair to request an opinion on a specific subject-matter. Moreover, the Chair of the EDPB is intended to be an independent position, and by requiring the Chair to request an opinion, the proposed text appears to undermine that independence. For this reason, we would prefer to go back to the first compromise text of the Presidency which referred to the issuance of guidelines in article 70(1)(hca) GDPR. However, we thank the Council Legal Service for its views expressed at the last meeting and will re-evalute accordingly. FI (Comments): FI can support the proposed Article 29a as well as recitals 27a and 27b. FI primarily supports that there are no changes to the definition of personal data.

Commission proposal	Drafting suggestions and Comments
	Considering the discussion in the Antici Group on 27 May, FI understands that there is a need to discuss this matter further, possibly in Coreper. FI primarily prefers to delete changes to the definition and that there are no implementing acts concerning pseudonymisation. FI supports the EDPB guidelines on the matter. Alternatively, FI can accept possible supplements to the definition of personal data that only codify the CJEU case law and do not change the current level of data protection. This is a redline for FI and FI cannot accept supplements that would go beyond the CJEU case law and would lead to attempts to circumvent the GDPR and would not bring clarity to smaller entities. Concerning the proposed Article 29a as well as recitals 27a and 27b, FI welcomes that the Presidency has unified the wording with the GDPR. It is important that the EDPB issues an opinion on pseudonymisation. FI can support the compromise proposal. FI supports that there are no implementing acts on pseudonymisation. Alternatively, FI can accept implementing acts but only acts that are technical in nature and/or would only "codify" the EDPB guidance on the matter (similarly as with data breach notification templates and high-risk lists). CZ (Drafting suggestions): **(27a) In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. The identification of a natural person should be assessed by the controller or the processor,**

Commission proposal	Drafting suggestions and Comments
	considering the actual technical, organisational and legal capabilities of the controller or processor. In light of the interpretation provided in the case-law of the Court of Justice of the European Union, it is important to provide further clarity on when a natural person should be considered to be identifiable following the application of pseudonymisation to personal data and the transmission to a recipient. ~~The European Data Protection Board should ensure consistency and support controllers by adopting an opinion on pseudonymisation and anonymisation, assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to apply pseudonymisation and anonymisation to personal data effectively and by clarifying circumstances whether and when the application of pseudonymisation to personal data may effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable. The opinion should also address the processing to be undertaken and other measures to be applied in order to effectively render personal data anonymous. It is important that the Board carries out a public consultation with relevant stakeholders prior to issuing its opinion.~~ While controllers remain fully responsible to determine and demonstrate whether pseudonymised data do not lead to re-identification of data subjects by persons other than the controller, the opinion should support and provide guidance to controllers regarding the effective application of pseudonymisation to personal data. CZ (Comments): **Red line:** **CZ does not agree with quasi-legislative role of the EDPB when comitology should be used.** **See comments on Art. 29a.**

Commission proposal	Drafting suggestions and Comments
	SK (Comments): **SK:** We propose to delete this recital. An explanation is provided in the comments to Article 29a. SE (Drafting suggestions): **In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. ~~The identification of a natural person should be assessed by the controller or the processor, considering the actual technical, organisational and legal capabilities of the controller or processor~~. In light of the interpretation provided in the case-law of the Court of Justice of the European Union, it is important to provide further clarity on when a natural person should be considered to be identifiable following the application of pseudonymisation to personal data and the transmission to a recipient. The European Data Protection Board should ensure consistency and support controllers by adopting an opinion on pseudonymisation and anonymisation, assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to apply pseudonymisation and anonymisation to personal data effectively and by clarifying circumstances whether and when the application of pseudonymisation to personal data may effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable. The opinion should also address the processing to be undertaken and other measures to be applied in order to effectively render personal data anonymous. It is important that the Board carries out a public consultation with relevant stakeholders prior to issuing its opinion. While controllers remain fully responsible to determine and demonstrate whether**

Commission proposal	Drafting suggestions and Comments
	pseudonymised data do not lead to re-identification of data subjects by persons other than the controller, the opinion should support and provide guidance to controllers regarding the effective application of pseudonymisation to personal data. SE (Comments): The wording of the sentence "***The identification of a natural person should be assessed by the controller or the processor, considering the actual technical, organisational and legal capabilities of the controller or processor."*** should be reconsidered or removed. The possibility to identify a natural person cannot be assessed solely in relation to the processor but also in relation to the controller, considering that the processor acts on behalf of the controller and should be assessed as a unit.
(27b) Pseudonymisation is one of the possible security measures within the meaning of Article 32 of Regulation (EU) 2016/679 and does not necessarily have to be applied in all cases. Whether pseudonymisation is appropriate, should be assessed on a case-by-case basis and depends on the context, the nature of the personal data and the existence of other appropriate technical and organisational measures. The effective application of pseudonymisation may also be clarified for controllers and processors through the approval of specific codes of conduct in accordance with Article 40 of Regulation (EU) 2016/679, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises.	NL (Comments): NL thanks the Presidency for adding recital 27b, in response to our previous amendment. FR (Comments): **Les autorités françaises peuvent soutenir les amendements apportés aux considérants 27a et 27b pour appuyer l'implication nécessaire du CEPD au soutien des responsables de traitements et des sous-traitants en matière de pseudonymisation effective. Les acteurs ont en effet besoin d'être accompagnés par une doctrine concrète, opérationnelle, effective et nourrie des retours des acteurs au travers de consultations préalables pour lui permettre de saisir les enjeux concrets du terrain.** **Concernant l'introduction d'une référence aux codes de conduites au considérant 27b, les autorités françaises rappellent néanmoins qu'à cet**

Commission proposal	Drafting suggestions and Comments
	égard, pour faciliter le développement de ces outils très chronophages, elles ont proposé des amendements ciblés qui permettraient à la Commission elle-même de proposer un code de conduite en la matière. Ceci permettrait de trouver un compromis juridiquement valide permettant de lui confier l'élaboration d'un outil opposable pour les opérateurs, dans le respect des procédures déjà prévues par le RGPD. EE (Comments): Estonia supports this amendment. AT (Comments): • AT **can support** the proposed Recital 27b. FI (Comments): See the comment above. CZ (Comments): CZ can accept this recital in the spirit of compromise but does not consider it a new solution or a solution effectively equivalent to implementing act on pseudonymisation.
(28) In order to assess whether **scientific** research ~~meets~~ **activities meet** the conditions of scientific research for the purpose of ~~this~~ Regulation **(EU) 2016/679**, account can be taken of elements such as **the purpose of the research, the** methodological ~~and systematic~~ approach **and ethical standards** applied **in the specific area** while conducting the research**, and adherence to the principles of transparency, reliability, accountability, oversight, verifiability, and rules for research integrity** ~~in the specific area~~. **Transparency may, among other things, involve making research**	NL (Drafting suggestions): (28) In order to assess whether scientific research activities meet the conditions of scientific research for the purpose of Regulation (EU) 2016/679, account can be taken of elements such as the purpose of the research, the methodological approach and ethical standards applied in the specific area while conducting the research, and adherence to the principles

Commission proposal	Drafting suggestions and Comments
results publicly available with due regard to legitimate limitations to access such as protection of intellectual property and trade secrets. Scientific research activities should be conducted autonomously and independently, free from undue pressure and contribute to the growth of society's general knowledge and wellbeing. This does not exclude that the outcome of scientific research activities may also aim to further commercial or private interests. **It is important that processing for scientific research activities prevent individuals from being subjected to harm or other adverse effects due to their participation in scientific** research and **respect, amongst others, human autonomy and, to the extent necessary, the notion of consent to participate in research should be used as a safeguard and is to be considered distinctively from consent under Regulation (EU) 2016/679. Scientific research can, amongst others, be part of and support innovation, such as** technology **or medical** development**. Scientific research activities may** ~~should~~ be conducted in academic, industry and other settings, **by public authorities or private entities,** including small and ~~medium-sized~~**medium sized** undertakings**. The outcome of scientific research may be applied for public interest, private or commercial purposes.** **The qualification of processing as being carried out for scientific research purposes**~~, (Article 179(2) TFEU) and~~ should be ~~always of a of high quality~~**assessed on a case-by-case basis, considering the objective characteristics of the research activity,** and should ~~adhere to the principles of principles of reliability, honesty, respect and accountability (verifiability~~**not rely solely on the declaration of the controller, nor undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU) 2016/679**.	of transparency, reliability, accountability, oversight, verifiability, and rules for research integrity. Transparency **should** ~~may~~, among other things, involve making research results publicly available with due regard to legitimate limitations to access such as protection of intellectual property and trade secrets. Scientific research activities should be conducted autonomously and independently, free from undue pressure and contribute to the growth of society's general knowledge and wellbeing. This does not exclude that the outcome of scientific research activities may also aim to further commercial or private interests. It is important that processing for scientific research activities prevent individuals from being subjected to harm or other adverse effects due to their participation in scientific research and respect, amongst others, human autonomy and, to the extent necessary, the notion of consent to participate in research should be used as a safeguard and is to be considered distinctively from consent under Regulation (EU) 2016/679. Scientific research can, amongst others, be part of and support innovation, such as technology or medical development. Scientific research activities may be conducted in academic, industry and other settings, by public authorities or private entities, including small and medium sized undertakings. The outcome of scientific research may be applied for public interest, private or commercial purposes. The qualification of processing as being carried out for scientific research purposes should be assessed on a case-by-case basis, considering the objective characteristics of the research activity, and should not rely solely on the declaration of the controller, nor undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU) 2016/679. **Scientific research applies the scientific method of observing phenomena, formulating and testing a hypothesis for those phenomena, and concluding as to the validity of the hypothesis. The notion of scientific research may not be stretched beyond its common meaning.** NL (Comments):

Commission proposal	Drafting suggestions and Comments
	This amendment tries to prevent that the clarification of the definition of scientific data would create a very liberal application or loophole in practice, which could be misused to undermine fundamental rights. Although the Presidency has added various improvements, NL is still concerned that the proposed definition is prone to abuse and that it extends the scope of exceptions for scientific research also in unintended ways. The wording of the two added sentences at the end is derived from the EDPB Opinion 1/2026, para. 9; EDPB Guidelines 03/2020, para. 10; EDPS Preliminary Opinion on data protection and scientific research (January 6, 2020), para. 3.2. Furthermore, NL proposes to adapt the second sentence of this recital to the proposed definition, which reads: "(…) producing verifiable and transparent results". Therefore, transparency *should* in principle involve that research results become publicly available. FR (Comments): **Si les autorités françaises peuvent accepter, à titre de compromis, le nouveau considérant 28, dont la rédaction provient dans l'ensemble de la version précédente du considérant 29, elles regrettent toutefois que la notion de concours à l'intérêt public de la recherche menée ait disparu de la définition elle-même à l'article 4.** EE (Comments): Estonia supports the amendment. AT (Comments): • AT **continues to have concerns** about the inclusion of a GDPR-specific definition of "scientific research".

Commission proposal	Drafting suggestions and Comments
	• The Recital should therefore be **deleted** (in line with proposed deletion of Art. 4(38)). Parts of this Recital could be moved to Recital 32, which also relates to scientific research. MT (Drafting suggestions): (28) In order to assess whether **scientific** research ~~meets~~ **activities meet** the conditions of scientific research for the purpose of ~~this~~ Regulation **(EU) 2016/679**, account can be taken of elements such as **the purpose of the research, the** methodological ~~and systematic~~ approach **and ethical standards** applied **in the specific area** while conducting the research**, and adherence to the principles of transparency, reliability, accountability, oversight, verifiability, and rules for research integrity** ~~in the specific area~~. **Transparency may, among other things, involve making research results publicly available with due regard to legitimate limitations to access such as protection of intellectual property and trade secrets. Scientific research activities should be conducted autonomously and independently, free from undue pressure and contribute to the growth of society's general knowledge and wellbeing. This does not exclude that the outcome of scientific research activities may also aim to further commercial or private interests.** **It is important that processing for scientific research activities prevent individuals from being subjected to harm or other adverse effects due to their participation in scientific** research and **respect, amongst others, human autonomy and, to the extent necessary, the notion of consent to participate in research should be used as a safeguard and is to be considered distinctively from consent under Regulation (EU) 2016/679. Scientific research can, amongst others, be part of and support innovation, such as** technology **or medical** development**. Scientific research activities may** ~~should~~ be conducted in academic, industry and other settings, **by public authorities or private entities,** including small and ~~medium-sized~~**medium sized** undertakings**.** ~~**The outcome of scientific**~~

Commission proposal	Drafting suggestions and Comments
	~~**research may be applied for public interest, private or commercial purposes.**~~ **The qualification of processing as being carried out for scientific research purposes,** ~~(Article 179(2) TFEU) and~~ should be ~~always of a of high quality~~**assessed on a case-by-case basis, considering the objective characteristics of the research activity,** and should ~~adhere to the principles of principles of reliability, honesty, respect and accountability (verifiability~~**not rely solely on the declaration of the controller, nor undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU) 2016/679**. MT (Comments): We believe that the following sentence is misleading and should be deleted: "*The outcome of scientific research may be applied for public interest, private or commercial purposes".* As stated in the definition of 'scientific research' and also in this recital, such research is conducted with the aim of contributing to the growth of society's general knowledge and wellbeing (which is essentially the public interest). In any event, **t**he recital already provides that the research may also aim to further commercial or private interests (in line with the EDPB Scientific Research Guidelines). FI (Comments): FI can support the proposed definition for scientific research as it includes all the necessary elements for scientific research. FI can support the recitals 28 and 32 which are balanced and consider both the public and private interests. CZ

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): (28) In order to assess whether **scientific** research ~~meets~~ **activities meet** the conditions of scientific research for the purpose of ~~this~~ Regulation **(EU) 2016/679**, account can be taken of elements such as ~~**the purpose of the research,**~~ **the** methodological ~~and systematic~~ approach **and ethical standards** applied **in the specific area** while conducting the research**, and adherence to the principles of transparency,** ~~**reliability, accountability, oversight,**~~ **verifiability, and rules for research integrity** ~~in the specific area~~. **Transparency may, among other things, involve making research results publicly available with due regard to legitimate limitations to access such as protection of intellectual property and trade secrets. Scientific research activities should** ~~**be conducted autonomously and independently, free from undue pressure and**~~ **contribute to the growth of society's general knowledge and wellbeing. This does not exclude that the outcome of scientific research activities may also aim to further commercial or private interests.** **It is important that processing for scientific research activities prevent individuals from being subjected to harm or other adverse effects due to their participation in scientific** research and **respect, amongst others, human autonomy and, to the extent necessary, the notion of consent to participate in research should be used as a safeguard and is to be considered distinctively from consent under Regulation (EU) 2016/679. Scientific research can, amongst others, be part of and support innovation, such as** technology **or medical** development**. Scientific research activities may** ~~should~~ be conducted in academic, industry and other settings, **by public authorities or private entities,** including small and ~~medium-sized~~**medium sized** undertakings**. The outcome of scientific research may be applied for public interest, private or commercial purposes.** **The qualification of processing as being carried out for scientific research purposes,** ~~(Article 179(2) TFEU) and~~ should be ~~always of a of high quality~~**assessed on a case-by-case basis, considering the objective**

Commission proposal	Drafting suggestions and Comments
	characteristics of the research activity, and should ~~adhere to the principles of principles of reliability, honesty, respect and accountability (verifiability~~**not rely solely on the declaration of the controller, nor undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU) 2016/679**. CZ (Comments): CZ: - purpose of the research should not be considered, only its nature, as any scientific research should be covered. For data protection legislation, it is fully sufficient that research is not illegal. Frequently, basic research has only the vaguest of purposes. However, this recital would force specification - and bureaucratic consideration - of its purpose. - the elements of "reliability, accountability and oversight" go above legal definition, are not explained and impute too bureaucratic nature to the research. It is not clear what "reliability" even means given the inherent uncertainty and falsifiability of science (as defined by Carl Popper). - The unclear terms "autonomously" and "independently", in an even more unclear context of "free from undue pressure" which might even add something more than "independently", should be either explained, including in the context of research by employees of private industrial enterprise, or deleted. It seems less complicated to simply delete these terms.
(29) It should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. In such cases it ~~is not~~**should not be** necessary to ascertain on the basis of Article 6(4) of ~~this~~ Regulation **(EU) 2016/679** whether the purpose of the further processing is compatible with the purpose for which the	LU (Comments): We consider that replacing "is not" by "should not be" does sufficiently clarify whether a combability test in application of Article 6(4) of the GDPR is necessary or not.

Commission proposal	Drafting suggestions and Comments
personal data are initially collected. **Such further processing should be considered compatible, provided that it is carried out in compliance with the principles and appropriate safeguards laid down in Regulation (EU) 2016/679, in particular Article 89.**	IT (Drafting suggestions): ***Scientific research activities should be conducted autonomously and independently, free from undue pressure and concur to public interest including safety, security, economic stability and well-being. It is important including safety, security, economic stability that scientific research activities prevent individuals from being subjected to harm or other adverse effects due to their participation in scientific research and respect, amongst others, human autonomy and the notion of consent to participate in research, which is to be considered distinctively from consent under Regulation (EU) 2016/679. Scientific research can, amongst others, support innovation, such as technology development. Scientific research activities may be conducted in academic, industry and other settings, by public authorities or private entities, including small and medium sized undertakings. The outcome of scientific research may be applied for public interest, private or commercial purposes.*** IT (Comments): It is proposed to add the following words, "including safety, security, economic stability," after "concur to public interest" to clarify that the concept of "public interest" is general in nature and can encompass different aspects of social life. It is also proposed to add the following sentence after the words "it is important": "It is important to define the notion of public interest as a general concept that is assessed on a case-by-case basis, even in the absence of a specific provision to identify it." This amendment, inspired by what has already been established in Italian case law regarding the processing of health data, has the advantage of allowing a case-by-case assessment, even in the absence of a law formally declaring the existence of a public interest as the purpose of the processing. The text should therefore be amended as follows (see second column)

Commission proposal	Drafting suggestions and Comments
	EE (Comments): Estonia supports the amendment. AT (Drafting suggestions): (29) It should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. In such cases it ~~is not~~***should not be*** necessary to ascertain on the basis of Article 6(4) of ~~this~~ Regulation ***(EU) 2016/679*** whether the purpose of the further processing is compatible with the purpose for which the personal data are initially collected. ***Such further processing should be considered compatible, provided that it is carried out in compliance with the principles and appropriate safeguards laid down in Regulation (EU) 2016/679, in particular Article 89.*** ***The qualification of processing as being carried out for scientific research purposes should be based on objective characteristics of the research activity and should not rely solely on the declaration of the controller, nor undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU) 2016/679. In order to assess whether scientific research activities meet the conditions of scientific research for the purpose of Regulation (EU) 2016/679, account can be taken of elements such as the purpose of the research, the methodological approach and ethical standards applied in the specific area while conducting the research, and adherence to the principles of transparency, reliability, accountability, oversight, verifiability, and rules for research integrity. Transparency may, among other things, involve making research results publicly available with due regard to legitimate limitations to access such as protection of intellectual property and trade secrets.*** ***Scientific research activities should be conducted autonomously and***

Commission proposal	Drafting suggestions and Comments
	independently, free from undue pressure and concur to public interest and well-being. It is important that scientific research activities prevent individuals from being subjected to harm or other adverse effects due to their participation in scientific research and respect, amongst others, human autonomy and the notion of consent to participate in research, which is to be considered distinctively from consent under Regulation (EU) 2016/679. Scientific research can, amongst others, support innovation, such as technology development. Scientific research activities may be conducted in academic, industry and other settings, by public authorities or private entities, including small and medium sized undertakings. The outcome of scientific research may be applied for public interest, private or commercial purposes. AT (Comments): • In line with the proposed deletion of Recital 27 and Art 4(38) the text should be **amended as proposed in the 2nd compromise text**. Explanations regarding the term 'scientific research' within the meaning of the GDPR would provide greater clarity and legal certainty. FI (Comments): FI can support this recital text. CZ (Comments): CZ supports this recital in a spirit of compromise.
~~(30) Trustworthy AI is key in providing for economic growth and supporting innovation with socially beneficial outcomes. The development and use of AI systems and the underlying models such as large language models and generative video models rely on data, including personal data, in~~	EE (Comments): Estonia supports deletion of this recital.

Commission proposal	Drafting suggestions and Comments
~~various phases in the AI lifecycle, such as the training, testing and validation phase and may in some instances be retained in the AI system or the AI model. The processing of personal data in this context may therefore be carried out for purposes of a legitimate interest within the meaning of Article 6 of Regulation (EU) 2016/679, where appropriate. This does not affect the obligation of the controller to ensure that the development or use (deployment) of AI in a specific context or for specific purposes complies with other Union or national law, or to ensure compliance where its use is explicitly prohibited by law. It also does not affect its obligation to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.~~	AT (Comments): AT **continues to support** the deletion.
~~(31) When the controller, in the light of the risk-based approach which informs the scalability of the obligations under this Regulation, is balancing the legitimate interest pursued by the controller or a third party and the interests, rights and freedoms of the data subject, consideration should be given to whether the interest pursued by the controller is beneficial for the data subject and society at large, which may for instance be the case where the processing of personal data is necessary for detecting and removing bias, thereby protecting data subjects from discrimination, or where the processing of personal data is aiming at ensuring accurate and safe outputs for a beneficial use, such as to improve accessibility to certain services. Consideration should also, among others, be given to reasonable expectations of the data subject based on their relationship with the controller, appropriate safeguards to minimise the impact on data subjects' rights such as providing enhanced transparency to data subjects, providing an unconditional right to object to the processing of their personal data, respecting technical indications embedded in a service limiting the use of data for AI development by third parties, the use of other state of the art privacy preserving techniques for AI training and appropriate technical measures to effectively minimise risks resulting, for example, from regurgitation, data leakage and other intended or foreseeable actions.~~	EE (Comments): Estonia supports deletion of this recital. AT (Comments): AT **continues to support** the deletion.

Commission proposal	Drafting suggestions and Comments
(32) The processing of personal data for scientific research purposes and the application of the GDPR's provisions on scientific research are conditional on the adoption of appropriate safeguards for the rights and freedoms of data subjects, pursuant to Article 89(1) GDPR. To that end, the GDPR balances the right to protection of personal data, pursuant to Article 8 CFREU, with the freedom of science, pursuant to Article 13 CFREU. The processing of personal data for the purpose of scientific research ~~therefore pursues a~~**can follow public interest within the meaning of Article 6(1)(e) of Regulation (EU) 2016/679 or be based on Member States and Union law. The processing of personal data for the purpose of scientific research may also be necessary for the purposes of the** legitimate ~~interest~~**interests pursued by a controller or by a third party** within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State law. This is without prejudice to the obligation of the controller to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.	EE (Comments): Estonia supports the amendment. AT (Comments): AT **continues to support** the proposed changes. FI (Comments): FI supports this recital text on scientific research. CZ (Drafting suggestions): (32) The processing of personal data for scientific research purposes and the application of the GDPR's provisions on scientific research are conditional on the adoption of appropriate safeguards for the rights and freedoms of data subjects, pursuant to Article 89(1) GDPR. To that end, the GDPR balances the right to protection of personal data, pursuant to Article 8 CFREU, with the freedom of science, pursuant to Article 13 CFREU. The processing of personal data for the purpose of scientific research ~~therefore pursues a~~**can follow public interest within the meaning of Article 6(1)(e) of Regulation (EU) 2016/679 or be based on Member States and Union law. The processing of personal data for the purpose of scientific research may also be necessary for the purposes of the** legitimate ~~interest~~**interests pursued by a controller or by a third party** within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State law. This is without prejudice to the obligation of the controller to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.

Commission proposal	Drafting suggestions and Comments
(33) The development of certain AI systems and AI models may involve the collection of large amounts of data, including personal data and special categories thereof. Special categories of personal data may **incidentally and** residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing **and while the controller did not initially envisage the processing of such personal data and has taken the appropriate technical and organisational measures to avoid such processing**. In order not to disproportionately hinder the development and operation of AI and taking into account the capabilities of the controller to identify and ~~remove~~**erase** special categories of personal data, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be allowed **for incidental and residual processing of special categories of data in the context of the development and operation of AI systems or AI models. The derogation should not be understood as covering the processing of special categories of personal data collected through prompts during the deployment of the AI system or AI models**. The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures during the entire lifecycle**, that is to say during the development and operation,** of an AI system or AI model and, once it identifies such data, effectively ~~remove them. If removal~~**erase them. If erasure** would **prove impossible or** require **manifestly** disproportionate effort, notably where the ~~removal~~ erasure of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, **or would be technically impossible,** the controller should effectively protect such data from **being further processed or processed for other purposes, in particular** being used to infer outputs, being disclosed or otherwise made available to third parties**. In line with the accountability principle, the controller should document its assessment and have processes in place to monitor and**	NL (Drafting suggestions): (33) The development of certain AI systems and AI models may involve the collection of large amounts of data**, which can contain ~~, including~~** personal data and special categories thereof**, subject to all requirements of Regulation (EU) 2016/679**. Special categories of personal data may incidentally and residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing and while the controller did not initially envisage the processing of such personal data and has taken the appropriate technical and organisational measures to avoid such processing. **Those measures should include filtering out, both at the collection stage – by avoiding collecting special categories of data in the first place – and immediately thereafter – by deleting or anonymising special categories of data prior to training AI models. ~~In order not to disproportionately hinder the development and operation of AI and t~~ T**aking into account the **technical** capabilities of the controller to **fully** identify and erase special categories of personal data, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be allowed for incidental and residual processing of special categories of data in the context of the development and operation of AI systems or AI models. **The derogation should remain limited to strictly incidental, unintentional and residual cases, where the processing does not rely on such special categories of personal data.** The derogation should not be understood as covering the processing of special categories of personal data collected through prompts during the deployment of the AI system or AI models. The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures during the entire lifecycle, that is to say during the development and operation, of an AI

Commission proposal	Drafting suggestions and Comments
demonstrate the effectiveness of these measures. This derogation should not apply where the processing of special categories of personal data is necessary for the purpose of the processing. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679 **or on other Union law, such as Regulation (EU) 2024/1689 regarding the processing of special categories of personal data for the purpose of ensuring bias detection and correction**. **The notion of AI system and AI model should be understood in the same manner as in Regulation (EU) 2024/1689.**	system or AI model and, once it identifies such data, effectively erase them. If erasure would prove **technically** impossible ~~**or require manifestly disproportionate effort**~~, ~~**notably where the erasure of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, or would be technically impossible**~~, the controller should effectively protect such data from being further processed or processed for other purposes, in particular being used to infer outputs, being disclosed or otherwise made available to third parties. In line with the accountability principle, the controller should document its assessment and have processes in place to monitor and demonstrate the effectiveness of these measures. This derogation should not apply where the processing of special categories of personal data is necessary for the purpose of the processing. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679 or on other Union law, such as Regulation (EU) 2024/1689 regarding the processing of special categories of personal data for the purpose of ensuring bias detection and correction. **Therefore, this derogation should for example not apply where special categories of personal data would be used for training objectives, evaluation, optimisation, bias testing, profiling, output generation, model improvement, or deployment.** The notion of AI system and AI model should be understood in the same manner as in Regulation (EU) 2024/1689. NL (Comments): NL has repeatedly proposed deletion of recital 33 because of the proposed deletion of the corresponding Article 9(2)(k). However, if a majority of the Member States supports this provision, NL considers it crucial that recital 33 is formulated in a more stringent manner, and that article 9(2)(k) and 9(5) should be strictly limited.

Commission proposal	Drafting suggestions and Comments
	As further explained in the comments below on those provisions, NL remains seriously concerned about the exception to the prohibition on processing special categories of personal data for "residual" data when training and using AI. In the current from, recital 33 reinforces these concerns by accepting that special category data may be retained in AI systems or models and by not emphasising prevention and erasure, but mitigation where removal is difficult. It is important to emphasise the need to avoid the presence of sensitive data and to avoid large-scale retention of sensitive data as a result of the proposed derogation. NL finds support in this in the guidance of the EDPB, which has noted that the safeguards "*should involve filtering data categories falling under Article 9(1) GDPR. The filtering should apply to both, data collection (for example, selecting criteria for what data is collected) and immediately after data collection (deleting data).*" (EDPB, Report of the work undertaken by the ChatGPT Taskforce, adopted on 23.05.2024, p 7, §19 and §17). EE (Comments): Estonia supports the amendments AT (Comments): AT **continues to support** the proposed changes. MT (Comments): In our last comments we had suggested that recital 33 should provide for the controllers' obligation to document its assessment of the impossibility or the manifestly disproportionate difficulty in deleting such special categories of data in line with the accountability principle. For this reason, we thank the Presidency for including the wording "*the controller should document its*

Commission proposal	Drafting suggestions and Comments
	assessment" in recital 33. However, we note that recital 33 and Article 3(3) of the Proposal still use the term "*operation*" which is not defined in the GDPR or the AI Act. For clarity, should this term be clarified or changed to "*deployment*"? FI (Comments): FI supports the derogation for AI-processing in Article 9 GDPR as well as the recital 33. FI can support the proposed text and safeguards. It is important that the derogation applies only to incidental and residual processing of special categories of personal data. CZ (Drafting suggestions): (33) The development of certain AI systems and AI models may involve the collection of large amounts of data, including personal data and special categories thereof. Special categories of personal data may **incidentally and** residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing **and while the controller did not initially envisage the processing of such personal data and has taken the appropriate technical and organisational measures to avoid such processing**. In order not to disproportionately hinder the development and operation of AI and taking into account the capabilities of the controller to identify and ~~remove~~**erase** special categories of personal data, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be allowed **for incidental and residual processing of special categories of data in the context of the development and operation of AI systems or AI**

Commission proposal	Drafting suggestions and Comments
	models. The derogation should not be understood as covering the processing of special categories of personal data collected through prompts during the deployment of the AI system or AI models. The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures during the entire lifecycle**, that is to say during the development and operation,** of an AI system or AI model and, once it identifies such data, effectively ~~remove them. If removal~~**erase them. If erasure** would **prove impossible or** require ~~**manifestly**~~ disproportionate effort, notably where the ~~removal~~ erasure of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, ~~**or would be technically impossible,**~~ the controller should effectively protect such data from **being** ~~**further processed or**~~ **processed for other purposes**~~**, in particular**~~ being used to infer outputs, being disclosed or otherwise made available to third parties**. In line with the accountability principle, the controller should document its assessment and have processes in place to monitor and demonstrate the effectiveness of these measures**. This derogation should not apply where the processing of special categories of personal data is necessary for the purpose of the processing. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679 **or on other Union law, such as Regulation (EU) 2024/1689 regarding the processing of special categories of personal data for the purpose of ensuring bias detection and correction**. **The notion of AI system and AI model should be understood in the same manner as in Regulation (EU) 2024/1689.** CZ (Comments): CZ: - "manifestly disproportionate effort " is something else than "disproportionate effort" used by the GDPR, and thus will add an

Commission proposal	Drafting suggestions and Comments
	unwarranted layer of uncertainty and complexity, rather than foster simplification. - If "technical impossibility" is a part of "impossibility", there is no need to refer to it specifically. - "Further processing" is distinguished from "processing for other purposes" thus clearly involves situations other than Art. 64) GDPR. In this wording, data are further processed even by storage and other operations under Art. 4(4) GDPR. Thus a recital requires contradictory duties – erasure is required, exception is created for impossible situations while inference or disclosure is prohibited, but storage is precluded as well. Either "further processed" should be deleted or the text should be brought in line with Art. 6(4) or 13(3) or 14(4) GDPR: "further processed for other purposes". - "in particular" is not correct logical operator here. As "further processing" in form of storage must be allowed, the really prohibited actions, such as inference or disclosure, must be prohibited in an exhaustive manner. BE (Comments): We oppose the change of *"the controller has not intented the processing of such personal data" to "the controller did not initially envisage the processing…".* This change weakens the requirement of "no intention". BE has a very strong preference for the original wording SE (Comments): Sweden can support this amendment.
(33a) The processing of personal data in the context of the development and deployment of an AI system or of an AI model, may be regarded as carried out for a legitimate interest of the controller concerned and be carried out in accordance with Article 6(1)(f) of Regulation 2016/679,	NL (Drafting suggestions): **(33a) [deleted]**

Commission proposal	Drafting suggestions and Comments
where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This does not affect the obligation of the controller to choose the most appropriate lawful ground of processing set out in Article 6 of Regulation (EU) 2016/679, such as Article 6(1)(e) with regard to processing by public authorities. Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model.	**If a majority of member states want to retain recital 33a, NL proposes the following amendments** (33a) The processing of personal data in the context of the development and deployment of an AI system or of an AI model, may be regarded as carried out for a legitimate interest of the controller concerned and be carried out in accordance with Article 6(1)(f) of Regulation 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. **It has to be recalled that the legal assessment of Article 6(1)(f) GDPR should be based on the existence of a legitimate interest, the necessity of processing, as the personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed and, balancing of interests. Fundamental rights and freedoms of data subjects on one hand and the controller's legitimate interests on the other hand have to be evaluated and balanced carefully. The reasonable expectations of data subjects should be taken into account in this assessment, which should include whether or not the personal data were publicly available, the nature of the relationship between the data subject and the controller and whether a link exists between the two, the nature of the service, the context in which the personal data was collected, the source from which the data were collected, the potential further uses of the model, and whether data subjects are actually aware that their personal data are online at all.** This does not affect the obligation of the controller to choose the most appropriate lawful ground of processing set out in Article 6 of Regulation (EU) 2016/679, such as Article 6(1)(e) with regard to processing by public authorities. Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure

Commission proposal	Drafting suggestions and Comments
	respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model. NL (Comments): NL strongly supports the deletion of the regulation of a legitimate interest basis specifically for AI (proposed Article 88c GDPR), and agrees with the objections previously raised by the presidency with regard to this article. NL thanks the Presidency for this deletion. However, in the new compromise proposal this subject is partly reintroduced in the form of a recital. NL is worried about this new recital 33a, because it could give the impression that this legal basis is given by default, without a necessity test and the associated balancing test of interests. Furthermore, it deviates from EDPB opinion 28/2024, because it fails to provide that the reasonable expectations of data subjects must be taken into account (the NL text proposal is derived from the factor the EDPB summed up on page 3 of the EDPB Opinion 28/2024). In recital article 33a is also missing that the legal assessment of Article 6(1)(f) GDPR should be based on the following criteria (three step test): i) existence of a legitimate interest, ii) necessity of processing, as the personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed and iii) balancing of interests. Fundamental rights and freedoms of data subjects on one hand and the controller's legitimate interests on the other hand have to be evaluated and balanced carefully. The reasonable expectations of data subjects should be taken into account in this assessment. LU (Comments): We welcome the reference indicating that the processing of personal data in the context of the development and deployment of an AI system may be

Commission proposal	Drafting suggestions and Comments
	regarded as carried out based on the controller's legitimate interest, even if this clarification appears only in the form of a recital. FR (Drafting suggestions): **The processing of personal data in the context of the development and deployment of an AI system or of an AI model, may be regarded as carried out for a legitimate interest of the controller concerned and be carried out in accordance with Article 6(1)(f) of Regulation 2016/679, where appropriate, except where other Union or national laws explicitly require consent, ~~and~~ or where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.** FR (Comments): **Les autorités françaises peuvent accepter le compromis de la Présidence d'intégrer le contenu de l'ancien article 88c au nouveau considérant 33a. Une clarification devrait toutefois être apportée : les situations dans lesquelles le consentement est la base légale, et celles dans lesquelles les intérêts des personnes, en particulier si elles sont vulnérables, doivent prévaloir, sont des situations distinctes et non cumulatives. Ainsi, ce n'est pas un « and » mais un « or » qu'il faudrait employer entre les deux propositions.** EE (Comments): Does this recital provide for the possibility to restrict/prohibit processing based on legitimate interest? If yes, then this should not be included only in the recital, but also in the articles. AT

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): (33a) The processing of personal data in the context of the development and deployment of an AI system or of an AI model, may be regarded as carried out for a legitimate interest of the controller concerned and be carried out in accordance with Article 6(1)(f) of Regulation 2016/679, where appropriate, except where other Union or national laws explicitly require consent, ~~**and**~~ **or** where such interests are overridden by the interests, or where fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This does not affect the obligation of the controller to choose the most appropriate lawful ground of processing set out in Article 6 of Regulation (EU) 2016/679, such as Article 6(1)(e) with regard to processing by public authorities. Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model. AT (Comments): • It should be made clear that the exceptions listed in Recital 33a are **alternative**, not cumulative - that is to say that, where Union or national law requires consent, Art 6(1)f cannot serve as legal basis, regardless of whether overriding third party interests exist or not. This could be achieved by using the conjunction **"or"** instead of "and". MT (Drafting suggestions): **(33a) The processing of personal data in the context of the development and deployment of an AI system or of an AI model, may be regarded as carried out for a legitimate interest of the controller concerned and be carried out in accordance with Article 6(1)(f) of Regulation 2016/679,**

Commission proposal	Drafting suggestions and Comments
	where appropriate, ~~except where other Union or national laws explicitly require consent,~~ and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This does not affect the obligation of the controller to choose the most appropriate lawful ground of processing set out in Article 6 of Regulation (EU) 2016/679, such as Article 6(1)(e) with regard to processing by public authorities. Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model. MT (Comments): We have no objections to including a recital providing that the legitimate interests of a controller may provide a legal basis pursuant to Article 6 GDPR for processing in the context of the development and deployment of an AI system, as long as it is clear that legitimate interests is not the preferred or only legal basis which could be relied upon in this context. In this regard, we positively note the sentence stating that this "*does not affect the obligation of the controller to choose the most appropriate lawful ground of processing set out in Article 6…".* However, the phrase "*except where other Union or national laws explicitly require consent*" in recital 33a might give rise to misinterpretations and we would prefer if this phrase is deleted. HU (Comments):
	HU: While we support preserving the technology-neutral structure of the GDPR and therefore understand the deletion of the former Article 88c, we would nevertheless welcome further clarification from the Presidency on how

Commission proposal	Drafting suggestions and Comments
	consistent legal certainty for AI developers and regulatory sandbox initiatives can be ensured on the basis of Recital 33a alone.
	FI (Comments): FI welcomes that the Presidency has introduced a new recital concerning AI-processing (recital 33a) and finds it important that the recital includes also the legal basis for public authorities. FI could have supported Article 88c with certain amendments, but this proposed new recital is a balanced compromise to bring legal clarity without adding a new Article. CZ (Drafting suggestions): **(33a) The processing of personal data in the context of the development and deployment of an AI system or of an AI model, may be regarded as carried out for a legitimate interest of the controller concerned and be carried out in accordance with Article 6(1)(f) of Regulation 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This does not affect the obligation of the controller to choose ~~the most~~ appropriate lawful ground of processing set out in Article 6 of Regulation (EU) 2016/679, such as Article 6(1)(e) with regard to processing by public authorities. Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model.**

Commission proposal	Drafting suggestions and Comments
	CZ (Comments): CZ prefers Article 88c because simple affirmation on AI in the normative text (that is not fully technologically neutral) is called for and would help EU AI academia and industry. CZ can be flexible in the spirit of compromise. There is no obligation for the controller under GDPR to chose "the most appropriate" lawful ground of processing. That is not surprising since some grounds may apply in parallel (as follows e.g. from Art. 17(1)(b) GDPR). A recital to this effect could not represent simplification in any conceivable manner. The controller is of course responsible for having appropriate lawful ground for processing, but we should not introduce more complexity. SE (Comments): SE is in favour of the proposed clarifications as regards the legal basis for the development and deployment of AI systems. ES (Comments): **Spain.** Regarding deletion of article 88 c and adding this recital 33.a, in spirit of compromise we can support the new recital 33.a. Our objectives are: • To expressly and legally recognize that legitimate interest can serve as the basis for processing personal data throughout the lifecycle of artificial intelligence systems and models, avoiding interpretive uncertainties and ex ante blocks that arise from a strict application of frameworks designed for traditional processing. • To define this use of legitimate interest through functional and weighting criteria linked to the design and operation of the system, without resorting to

Commission proposal	Drafting suggestions and Comments
	closed lists of purposes or rigid technical requirements that would limit innovation or quickly become obsolete. • To adapt the application of the GDPR to the technical reality of advanced artificial intelligence systems, particularly those of high complexity or generative nature, in which classic mechanisms for immediate individual control are not always viable or verifiable. • Guarantee effective protection of rights, such as the right to object when it becomes an obligation to comply, by reorienting the exercise of rights like the right to object towards structural, verifiable solutions that are proportionate to the actual impact of the processing. • Allow public sector authorities and bodies to also rely on legitimate interest for the processing of personal data related to the development and use of artificial intelligence systems, even when acting in the exercise of their functions, without requiring specific legal authorization, subject to the requirements and safeguards provided for in the provision.
(34) **Processing of** biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. The notion of biometric ~~data~~**recognition** includes two distinct functions, namely the identification of a natural person or the verification (also called 'authentication') of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of ~~the~~ Regulation **(EU) 2016/679** should ~~also~~ be allowed where the verification of the claimed identity of the data subject is necessary for a purpose pursued by the controller~~,~~ and**, where**	LU (Comments): Regarding "biometric recognition", we would be cautious to introduce a new, non-defined notion into the GDPR. IT (Drafting suggestions): *The notion of biometric* ***~~recognition~~ identification*** *includes two distinct functions, namely the identification of a natural person or the verification*

Commission proposal	Drafting suggestions and Comments
applicable, subject to appropriate safeguards laid down under Union law or Member States law in accordance with Article 9(4) of Regulation (EU) 2016/679. Where biometric data are processed for the purpose of confirming the identity of a data subject, controllers should, where possible, prioritise authentication methods that do not involve the processing of biometric data. The controller should choose from equally effective means the less intrusive one. The processing of biometric data for identity verification should therefore only be used where necessary and proportionate and subject to appropriate safeguards. For the purposes of this Regulation, biometric identification should be understood as the processing of biometric data through comparison against a database intended to determine the identity of a natural person, whereas biometric verification refers to a one-to-one comparison used solely to confirm a claimed identity. This derogation should apply where suitable safeguards apply to ~~enable the data subject to have~~**ensure that the biometric data or the means needed for the verification are under the** sole control of the **data subject. Sole control means that the data subject can effectively decide when and how his or her biometric data are used for** verification**, without the controller having the technical capacity to access such biometric data in decrypted form or** process **them outside the strictly limited comparison process necessary for verification**. For example, **this is the case** where the biometric data are securely stored solely at the ~~side~~**device** of the data subject or are securely stored ~~at the side of~~**by** the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is **securely** held solely by the data subject, ~~that~~**and subject to measures ensuring the overall security of** processing ~~is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the~~**, including during the enrolment phase of data subject's** biometric data ~~or only for a very limited time~~**and** during the verification process. **Such verification may in particular be required in the context of electronic identification systems and trust services under Union law. Other examples of appropriate**	*(also called 'authentication') of his or her claimed identity, both of which rely on different technical processes.* ***The mere processing of biometric data, which only enables a natural person to be recognised without their name or other identifying information being known, should not be considered identification. For further clarification, the processing of biometric data that is not linked to a legal identity attributed by a state should not be considered identification*** IT (Comments): It should be clarified that the GDPR applies to the processing of biometric data for identification purposes, not recognition. This would allow the use of biometric data for private security purposes, making it possible, for example, to identify an individual authorized to access certain areas without identifying them (i.e., without also acquiring their personal details and other identifying data). In other words, given that it is possible to recognize an individual without necessarily knowing who they are, this distinction should be clarified. The text should be amended as follows: see second column **Article 9(2)** **Accordingly, Article 9(2) should be amended by adding the following sentence after the last paragraph:***The mere processing of biometric data, which only enables a natural person to be recognised without their name or other identifying information being known, should not be considered identification.* EE (Comments): Estonia supports the amendment. AT

Commission proposal	Drafting suggestions and Comments
safeguards are ensuring that end-to-end encryption is used when data are transmitted over a communication channel and providing data subjects with the possibility to securely erase their biometric data at any time.	(Comments): • The proposed changes in the recital introduce new terms like biometric *recognition* while Article 9(2)(l) uses the term *verification*. For the sake of clarity, the language of the recital should be aligned with the language used in the operational part in order to prevent creating new notions in the recital which are neither used nor defined in the binding part of the GDPR and avoid misunderstandings. FI (Comments): Concerning the derogation for biometric verification in Article 9 GDPR [Art 3(3)(a) Digiomnibus], FI would have preferred to harmonise this matter in the GDPR, complemented with additional safeguards. FI can show flexibility in this (not a redline), although this proposal does not support the aim to simplify. If majority supports this proposal, FI can accept it. FI can support this recital text. CZ (Drafting suggestions): (34) **Processing of** biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. The notion of biometric ~~data~~**recognition** includes two distinct functions, namely the identification of a natural person or the verification (also called **'**authentication**'**) of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of ~~the~~ Regulation **(EU) 2016/679**

Commission proposal	Drafting suggestions and Comments
	should ~~also~~ be allowed where the verification of the claimed identity of the data subject is necessary for a purpose pursued by the controller~~,~~ and**, where applicable, subject to appropriate safeguards laid down under Union law or Member States law in accordance with Article 9(4) of Regulation (EU) 2016/679.** ~~**Where biometric data are processed for the purpose of confirming the identity of a data subject, controllers should, where possible, prioritise authentication methods that do not involve the processing of biometric data.**~~ **The controller should choose from equally effective means the less intrusive one. The processing of biometric data for identity verification should therefore only be used where necessary and proportionate and subject to appropriate safeguards. For the purposes of this Regulation, biometric identification should be understood as the processing of biometric data through comparison against a database intended to determine the identity of a natural person, whereas biometric verification refers to a one-to-one comparison used solely to confirm a claimed identity. This derogation should apply where** suitable safeguards apply to ~~enable the data subject to have~~**ensure that the biometric data or the means needed for the verification are under the** sole control of the **data subject. Sole control means that the data subject can effectively decide when and how his or her biometric data are used for** verification**, without the controller having the technical capacity to access such biometric data in decrypted form or** process **them outside the strictly limited comparison process necessary for verification**. For example, **this is the case** where the biometric data are securely stored solely at the ~~side~~**device** of the data subject or are securely stored ~~at the side of~~**by** the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is **securely** held solely by the data subject, ~~that~~**and subject to measures ensuring the overall security of** processing ~~is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the~~**, including during the enrolment phase of data subject's** biometric data ~~or only for a very limited time~~**and** during the verification process. **Such verification may in**

Commission proposal	Drafting suggestions and Comments
	particular be required in the context of electronic identification systems and trust services under Union law. ~~**Other examples of appropriate safeguards are ensuring that end-to-end encryption is used when data are transmitted over a communication channel and providing data subjects with the possibility to securely erase their biometric data at any time.**~~ CZ (Comments): CZ welcomes the phrase "where applicable", **which is a red line**. Moreover, - The fifth sentence is deleted since restricting usage of biometric verification to necessary cases is not compatible with everyday experience (smartphones are opened by biometric verification many times a day). - The last sentence is deleted since additional safeguards not required by GDPR (e.g. the encryption, let alone its specific forms, are never required by GDPR) cannot be introduced by recital either. SE (Comments): Sweden has previously stressed that the addition of "s**ubject to appropriate safeguards laid down under Union or Member States law."** could risk of causing a fragmented application within the internal market and could therefore be reconsidered. The reference to article 9.4 GDPR is positive step to ensure foreseeability in this regard. ES (Comments): **Spain.** We want to add the following safeguards: Biometric technologies must enable the generation of multiple templates without allowing any of them to

Commission proposal	Drafting suggestions and Comments
	be derived from one another, thereby ensuring they can be revoked and renewed as many times as necessary, similarly to traditional passwords. Additionally, the biometric technologies used must guarantee irreversibility, meaning it must be impossible to reconstruct the original biometric sample from the template stored on the user's device or database. They must also ensure inter-system privacy (anti-cross-matching); that is, allowing the same biometric trait to be used across different systems without enabling those systems to cross-reference their databases to track the user. Given the rapidly evolving nature of these technologies, the EDPB will develop guidelines for the appropriate use of biometric technologies in alignment with the GDPR.
(35) **Chapter III of Regulation (EU) 2016/679 sets out rights of the data subject and corresponding obligations of the controller. Inter alia,** Article 15 of Regulation (EU) 2016/679 provides data subjects with the right to obtain **confirmation** from the controller ~~confirmation~~ as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and certain additional information. The right of access should allow the data subject to be aware of, and to verify, the lawfulness of the processing and enable him or her to exercise his or her other rights under Regulation (EU) 2016/679. ~~By contrast, it should be clarified in~~ Article 12 **(5) of that** ~~of the~~ Regulation **already provides that where the request to exercise a** ~~that the~~ right ~~of access, which is from the outset favourable to data subjects,~~**under Regulation 2016/679 is manifestly unfounded or excessive, the controller may either charge a reasonable fee or refuse to act on the request. The controller** should ~~not be abused in the sense that~~**provide** the data ~~subjects abuse them for purposes other than the protection of their data~~**subject with the reason thereof. A request is also to be considered excessive where an abusive intention on the part of the data subject submitting those requests can be demonstrated by the controller**. For example, such an ~~abuse of the right of access~~**abusive intention** would arise where the data subject ~~intends to cause the controller to refuse an access request, in order to subsequently demand the payment of~~	EE (Comments): Estonia supports the amendment AT (Comments): • AT **welcomes the further clarification** and thanks the Presidency for the consideration. FI (Comments): FI thanks the Presidency for mentioning public authorities in the recital. This is important for us – it should be clear that also public authorities have the means to address malicious intentions to adversely affect public authorities' work for instance by utilising AI agents for repeated/endless requests. If possible, FI repeats it proposal ("for instance by utilising AI agents for malicious automated requests") that could be added at the end of the recital but can support this recital text as well.

Commission proposal	Drafting suggestions and Comments
~~compensation, potentially under the threat of bringing a claim for damages. Other examples of abuse include situations where data subjects make~~**submits** excessive ~~use of the right of access~~**numbers of identical or largely similar requests** with the ~~only~~**sole** intent of causing damage or harm to the controller ~~or when~~**. Repeated requests are not automatically excessive in nature but may indicate an abusive intent on the part of the data subject. Other examples include situations where** an individual ~~makes~~**submits** a request, but at the same time offers to withdraw it in return for some form of benefit from the controller~~. Moreover, in order to keep their burden to a reasonable extent, controllers should bear a lower burden of proof regarding the excessive character of~~**, when an subject submits** a request ~~than regarding the manifestly unfounded character of a request. The reason is that the manifestly unfounded character of a request depends on facts that lie principally within the controller's sphere of responsibility, whereas the excessive character of a request concerns the possibly abusive conduct of a data subject,~~**with the sole purpose of obtaining compensation for an alleged infringement** which ~~lies primarily outside the controller's sphere of influence, and therefore the controller may be able to prove such abuse only to a reasonable level. In any event, while requesting access under Article 15 of Regulation (EU) 2016/679~~**is deliberately provoked by** the data subject ~~should be as specific as possible. Overly broad and undifferentiated requests should also be regarded as excessive~~**, or when the exercise of a right is made with the intention to adversely affect a judicial procedure or with deliberate intention to adversely affect and burden public authorities**.	CZ (Comments): CZ does not make specific proposal but still believes that only return to original Commission proposal of Art. 12(5), i.e. "reasonable grounds to believe" would have practical impact on the position of controllers. SI (Comments): The recital lays down examples of access requests that may be considered "abusive"; however, it does not define examples of access requests or types of conduct that should not be regarded as "abusive". This creates an imbalanced approach and entails a certain degree of risk for the effective exercise of a broad range of fundamental rights. We therefore propose to add a clarification that the assessment of whether a request for access to data is "abusive" must not prejudice the exercise of individuals' fundamental rights, and that the recital should include illustrative examples of situations that are not to be regarded as "abusive". SE (Comments): To Sweden, it is essential to ensure that proposed amendment corresponds to need of controllers while safeguarding an effective protection on behalf of the data subjects. It should be considered whether the deletion of a lower burden of proof in this regard could risk of hindering a real alleviation on behalf of the controllers. We therefore suggest to keep the Commission's proposal with regards to the proposed alleviation of burden.
(35a) Article 57 of Regulation (EU) 2016/679 provides rules for situations where requests from a data subject to the supervisory authority, including complaints under Article 77 of Regulation (EU)	EE (Comments): Estonia supports the amendment

Commission proposal	Drafting suggestions and Comments
2016/679, are manifestly unfounded or excessive, in particular because of their repetitive character. Articles 12 and 57 of Regulation (EU) 2016/679 use the same wording and pursue the same objective, namely to provide for an exception to the free-of-charge principle applicable to the tasks carried out by the supervisory authorities and the exercise of rights of the data subject, respectively. In order to reduce the burden of controllers with regard to excessive requests, which may also occur in relation to requests, including complaints, to the supervisory authority concerning the controller, the notion of excessiveness in Article 57 of Regulation (EU) 2016/679 should be adapted likewise.	AT (Comments): AT **continues to support** the inclusion of Recital 35a. In light of the recent ruling by the ECJ in Case No. 526/24 (*Brillen Rotter*) we would put it to the Presidency to consider whether the text could be amended to further clarify that repeated complaints are not automatically excessive in nature but may indicate an abusive intent on the part of the complainant. This may be achieved by striking the example of repetitiveness as a case of excessive complaints. FI (Comments): FI supports the proposed recital 35a and Article 57(4) GDPR [Art. 3(11) Digiomnibus] concerning data protection authorities' (DPA) possibilities to refuse manifestly unfounded and excessive requests as well. CZ (Comments): CZ is positive to the spirit of this recital and would support change of Art. 57 similarly to original Commission proposal to amend Art. 12(5). SE (Comments): No comments.
(36) Article 13 of Regulation (EU) 2016/679 requires the ~~data~~ controller to provide the data subject with certain information on the processing of his or her personal data as well as certain further information necessary to ensure fair and transparent processing, as defined in paragraphs 1, 2 and 3 of that	LU (Comments):

Commission proposal	Drafting suggestions and Comments
provision. According to paragraph 4 of Article 13 of Regulation (EU) 2016/679, that obligation does not apply where and insofar as the data subject already has the information. To further reduce the burden of ~~data~~ controllers, without undermining the possibilities of the data subject to exercise his or her rights under Chapter III of ~~the~~**that** Regulation, this derogation should be extended to situations **where the personal data have been collected in the context of a clear and circumscribed relationship between a data subject and a controller exercising an activity that does not involve processing a large amount of personal data,** where the processing is not likely to result in a high risk, within the meaning of Article 35 of ~~the~~**that** Regulation, and there are reasonable grounds to ~~assume~~**believe** that the data subject already has the information referred to in points (a) and (c) of paragraph 1 **of Article 13** in the light of the context in which the personal data have been collected~~, in particular regarding the~~**. A clear and circumscribed** relationship ~~between data subjects and the controller. These should be the situations where the context of the relationship between~~**requires** the controller and the data subject ~~is very clear and circumscribed and the controller's activity is not data intensive,~~**to have a direct relationship** such as the relationship between a craftsman and their clients**. The application of the derogation from the information obligation should not undermine the principle of transparency and should be limited to situations where the controller has reasonable grounds to believe that the data subject already possesses the required information. These should be the situations where the personal data are collected in the context of a direct and clearly circumscribed relationship between data subjects and a controller and does not involve the processing of a large amount of personal data**, **and** where the scope of processing is limited to the minimum data necessary to perform the service. ~~The controller's activity is not data intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment.~~ In such ~~circumstances, that is to say when the processing is non data intensive, non complex and where~~	The terminology uses in this recital seems to vary since reference is made to a "*clear and circumscribed relationship*" but also to a "*direct and clearly circumscribed relationship*". EE (Comments): Estonia supports the amendment AT (Drafting suggestions): (36) Article 13 of Regulation (EU) 2016/679 requires the data controller to provide the data subject with certain information on the processing of his or her personal data as well as certain further information necessary to ensure fair and transparent processing, as defined in paragraphs 1, 2 and 3 of that provision. According to paragraph 4 of Article 13 of Regulation (EU) 2016/679, that obligation does not apply where and insofar as the data subject already has the information. To further reduce the burden of data controllers, without undermining the possibilities of the data subject to exercise his or her rights under Chapter III of ~~the~~***that*** Regulation, this derogation should be extended to situations ***where the personal data have been collected in the context of a clear and circumscribed relationship between a data subject and a controller exercising an activity that does not involve large scale ~~the~~ processing ~~a large amount~~ of personal data,*** where the processing is not likely to result in a high risk, within the meaning of Article 35 of ~~the~~***that*** Regulation, and there are reasonable grounds to ~~assume~~***believe*** that the data subject already has the information referred to in points (a) and (c) of paragraph 1 ***of Article 13*** in the light of the context in which the personal data have been collected~~, in particular regarding the~~***. A clear and circumscribed*** relationship ~~between data subjects and the controller. These should be the situations where the context of the relationship between~~***requires*** the controller and the data subject ~~is very clear and circumscribed and the controller's activity is not data intensive,~~***to have a***

Commission proposal	Drafting suggestions and Comments
~~the controller collects a low amount of personal data~~**cases**, it should be reasonable to expect, for instance, that the data subject has the information on the identity and contact details of the controller**,** as well as on the purpose of ~~the~~ processing ~~when that processing is carried out for the performance of a contract to which a data subject is a party, or when the data subject has given his or her consent to that processing, in accordance with the requirements laid down in Regulation (EU) 2016/679~~.- The same should apply**, under the aforementioned conditions,** to associations and sport clubs where the processing of personal data is confined to the management of membership, communication with members and the organisation of activities. Nevertheless, this derogation from the obligations of Article 13 is without prejudice to the independent obligations of the controller under Article 15 of that Regulation, which applies in case the data subject requests access based on the latter provision. **This derogation should only apply to processing operations which are foreseeable and non-complex, which is not the case in the field of employment or in relations with public authorities or public bodies or private entities for the performance of a task in the public interest.** Where the derogation from the obligations of Article 13 does not apply, in order to balance the need for completeness and easy understanding by the data subject, controllers may adopt a layered approach when providing the information required, notably by allowing users to navigate to further information.	***direct relationship*** such as the relationship between a craftsman and their clients. ***The application of the derogation from the information obligation should not undermine the principle of transparency and should be limited to situations where the controller has reasonable grounds to believe that the data subject already possesses the required information. These should be the situations where the personal data are collected in the context of a direct, limited and clearly circumscribed relationship between data subjects and a controller and does not involve large scale ~~the~~ processing ~~of a large amount~~ of personal data, and*** where the scope of processing is limited to the minimum data necessary to perform the service. ~~The controller's activity is not data-intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment.~~ In such ~~circumstances, that is to say when the processing is non-data-intensive, non-complex and where the controller collects a low amount of personal data~~***cases***, it should be reasonable to expect, for instance, that the data subject has the information on the identity and contact details of the controller***,*** as well as on the purpose of ~~the~~ processing ~~when that processing is carried out for the performance of a contract to which a data subject is a party, or when the data subject has given his or her consent to that processing, in accordance with the requirements laid down in Regulation (EU) 2016/679~~.- The same should apply***, under the aforementioned conditions,*** to associations and sport clubs where the processing of personal data is confined to the management of membership, communication with members and the organisation of activities. Nevertheless, this derogation from the obligations of Article 13 is without prejudice to the independent obligations of the controller under Article 15 of that Regulation, which applies in case the data subject requests access based on the latter provision. ***This derogation should only apply to processing operations which are foreseeable and non-complex, which is not the case in the field of employment or in relations with public authorities or public bodies or private entities for the performance of a task in the public interest.*** Where the derogation from the obligations of Article

Commission proposal	Drafting suggestions and Comments
	13 does not apply, in order to balance the need for completeness and easy understanding by the data subject, controllers may adopt a layered approach when providing the information required, notably by allowing users to navigate to further information. AT (Comments): • AT **can support** the compromise proposal on Article 13(4) and Recital 36 GDPR. The proposed amendments provide important clarifications. • We would still prefer the use of the term "**large scale processing of personal data**" as that term is already used in the GDPR, notably in Article 35 – which the proposed Article 13(4) itself refers to – as well as Article 37, and covered by relevant EDPB guidelines. • Alternatively, we would ask the Presidency for the reasoning for using the term "processing of large amounts of personal data" instead of "large scale processing of personal data". FI (Comments): FI can support this recital text.
(37) Where the **further** processing **by the same controller** takes place for the purpose of scientific research and the provision of information to the data subject proves to be impossible or would involve a disproportionate effort it should not be necessary to provide the information provided for under Article 13 of this Regulation. The controller should make reasonable efforts to acquire contact details if they are readily available and acquisition would not require a disproportionate effort. The provision of the information would involve a disproportionate effort in particular where the controller at the time of collection of the personal data did not know or anticipate that it would process personal data for scientific research purposes at a later stage, in which case it may not have easily available contact details of the data subjects. In such situations the controller should inform data subjects	IT (Drafting suggestions): *Where the further processing by the same controller takes place for the purpose of* ***medical and*** *scientific research* ***and technological applications it should not be necessary to provide the information provided for under Article 13 of this Regulation*** ~~*, and the provision of information to the data subject proves to be impossible or would involve a disproportionate effort*~~*.* IT (Comments): **Article 6**

Commission proposal	Drafting suggestions and Comments
indirectly, such as by making the information publicly available. The provision of such information should ensure that as many data subjects concerned as possible are reached. Relevant means to make the information publicly available should be determined depending on the context of the research project and the data subjects involved.	Consequently, Article 6 should be replaced as follows:*In Article 13, paragraph 5 t* *Where the further processing by the same controller takes place for the purpose o and scientific research and technological applications it should not be necessary t the information provided for under Article 13 of this Regulation.* *In such cases the controller shall take appropriate measures to protect the data rights and freedoms and legitimate interests, including making the information available.'* EE (Comments): Estonia supports the amendment. FI (Comments): FI can support this recital text. SE (Comments): See comments below in relation to Article 13(5).
(38) Article 22 of Regulation (EU) 2016/679 provides ~~for~~**that data subject has the right not to be subject to a decision based solely on automated processing, except when specific conditions are met and in accordance with** rules governing the processing of personal data when the ~~data~~ controller makes decisions which have legal effects **concerning the data subject** or similarly significant effects on the data subject, based solely on automated processing. In order to provide greater legal certainty, it should be clarified that ~~decisions~~**when assessing whether a decision** based solely on automated processing ~~are allowed when specific conditions are met, as set out in Regulation (EU) 2016/679. It should also be clarified that when~~	LU (Comments): Article 22 of the GDPR has long been regarded as offering limited legal clarity and is frequently perceived as difficult to understand in practice. Moreover, the concrete legal result of an explicit reference to a 'right' not to be subject to an automated decision remain uncertain, a point clearly reflected in the ongoing debate surrounding this provision. We would be more favourable to the initial proposal of the Commission. EE

Commission proposal	Drafting suggestions and Comments
~~assessing whether a decision~~ is necessary for entering into, or performance of, a contract between the data subject and a ~~data~~ controller, as set out in Article 22(2)(a) of Regulation (EU) 2016/679, it should not be required that the decision could be taken only by solely automated processing. ~~This means that~~ The fact that the decision could also be taken by a human does not prevent the controller from taking the decision by solely automated processing**.** When several equally effective automated processing solutions exist, the controller should use the less intrusive one.	(Comments): Estonia supports the amendment AT (Comments): • AT continues to find it **problematic to determine** the meaning of the term "**necessary**" for the entering into or performance of a contract in accordance with Article 22 (1)a. This issue is currently the subject of a case pending before the CJEU (Case C-568/25). The CJEU should not be pre-empted in this regard. MT (Drafting suggestions): (38) Article 22 of Regulation (EU) 2016/679 provides ~~for~~**that data subject has the right not to be subject to a decision based solely on automated processing, except when specific conditions are met and in accordance with** rules governing the processing of personal data when the ~~data~~ controller makes decisions which have legal effects **concerning the data subject** or similarly significant effects on the data subject, based solely on automated processing. In order to provide greater legal certainty, it should be clarified that ~~decisions~~**when assessing whether a decision** based solely on automated processing ~~are allowed when specific conditions are met, as set out in Regulation (EU) 2016/679. It should also be clarified that when assessing whether a decision~~ is necessary for entering into, or performance of, a contract between the data subject and a ~~data~~ controller, as set out in Article 22(2)(a) of Regulation (EU) 2016/679, it should not be required that the decision could be taken only by solely automated processing. ~~This means that~~ The fact that the decision could also be taken by a human does not prevent the controller from taking the decision by solely automated processing**.** ~~**When several equally effective automated processing solutions exist, the controller should use the less intrusive one.**~~ **However, the controller needs to be able to show that the processing is necessary**

Commission proposal	Drafting suggestions and Comments
	and that no less privacy-intrusive means (automated or otherwise) could be adopted. MT (Comments): We agree with the recommendation made in paragraph 72 of the EDPB-EDPS Joint Opinion 2/2026 that the text should clarify that automated decision-making covered by Article 22(1) GDPR is only 'necessary' if no other equally effective and less intrusive means (automated or not) are available to the controller. We do not consider this to be adequately captured by the last sentence of recital 38 and therefore suggest an alternative wording. FI (Comments): FI can support this recital text. CZ (Comments): CZ fully supports this recital but believes that clarification should be reflected in the legal text as well. SE (Comments): The recital provides for a more generous approach than the text in operative part. The exception described in the Article seems to stipulate that automated decision making must be strictly necessary for the exception to apply. The wording of the recital on the other hand states that fact that the decision can be taken by a human does not preclude the possibility of automated decision making. Sweden considers that the operative text should be changed to reflect the wording of the recital.

Commission proposal	Drafting suggestions and Comments
(39) ~~In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should be aligned with that of communication of a personal data breach to the data subject under Article 34 of that Regulation.~~ In the case of a data breach that is not likely to result in a high risk to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should ~~prepare~~**establish and make public** a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person~~.~~ ~~The Commission should take due account of the proposal prepared by the Board and review them, as necessary, prior to adoption~~**, and a common list of circumstances in which a personal data breach does not result in such a high risk**. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated **where necessary. The Commission may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates** where necessary. The lack of a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches. **The alignment of notification thresholds should not affect the controller's obligation to carry out an individual risk assessment and to maintain complete documentation of personal data breaches in accordance with Article**	NL (Drafting suggestions): (39) In the case of a data breach that is not likely to result in a high risk to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should establish and make public a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person, and a common list of circumstances in which a personal data breach does not result in such a high risk. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated where necessary. ~~**The Commission may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates where necessary.**~~ The lack of a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches. The alignment of notification thresholds should not affect the controller's obligation to carry out an individual risk assessment and to maintain complete documentation of personal data breaches in accordance with Article 33(5) and Article 30 of Regulation (EU) 2016/679. The common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedom of a natural person should also apply in order to determine when communicating the data breaches to the data subject, in accordance with Article 34.

Commission proposal	Drafting suggestions and Comments
33(5) and Article 30 of Regulation (EU) 2016/679. The common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedom of a natural person should also apply in order to determine when communicating the data breaches to the data subject, in accordance with Article 34.	NL (Comments): NL refers to its amendment on Article 33(6). EE (Drafting suggestions): (39) ~~In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should be aligned with that of communication of a personal data breach to the data subject under Article 34 of that Regulation.~~ In the case of a data breach that is not likely to result in ~~a high~~ an impactful risk to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should ~~prepare~~establish and make public a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in ~~a high~~ an impactful risk to the rights and freedoms of a natural person~~. The Commission should take due account of the proposal prepared by the Board and review them, as necessary, prior to adoption~~, and a common list of circumstances in which a personal data breach does not result in such a high risk. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated where necessary. ~~The Commission may adopt, by means of an~~

Commission proposal	Drafting suggestions and Comments
	~~implementing act, the common template as established by the Board, as well as its updates where necessary.~~ The lack of a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches. The alignment of notification thresholds should not affect the controller's obligation to carry out an individual risk assessment and to maintain complete documentation of personal data breaches in accordance with Article 33(5) and Article 30 of Regulation (EU) 2016/679. The common list of circumstances in which a personal data breach is likely to result in ~~a high~~ an impactful risk to the rights and freedom of a natural person should also apply in order to determine when communicating the data breaches to the data subject, in accordance with Article 34. EE (Comments): Estonia supports reducing unnecessary data breach notifications, but notes that controllers might underestimate their impact on data subjects. Multiple low-risk breaches, when combined, could pose higher risks to individuals' rights and DPAs should be made aware of those. We recommend using terms like "impactful risks" or "increased risks." While we acknowledge the effort to provide a solution to the situation that the list adopted by EDPB might be challenged in the ECJ, we would like to avoid the diminishing of EDPB's autonomy. For this reason, we suggest removing the clauses that permit the Commission to adopt implementing acts AT (Drafting suggestions): (39) ~~In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should be aligned with that of communication of a personal data~~

Commission proposal	Drafting suggestions and Comments
	~~breach to the data subject under Article 34 of that Regulation.~~ In the case of a data breach that is not likely to result in ~~a high risk~~**an "impactful risk" ["relevant risk"/"increased risk"]** to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should ~~prepare~~***establish and make public*** a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in ~~a high risk~~ **an "impactful risk" ["relevant risk"/"increased risk"]** to the rights and freedoms of a natural person~~. The Commission should take due account of the proposal prepared by the Board and review them, as necessary, prior to adoption~~***, and a common list of circumstances in which a personal data breach does not result in such ~~a high risk~~*** **an "impactful risk" ["relevant risk"/"increased risk"]**. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated ***where necessary. The Commission may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates*** where necessary. The lack of a common list of circumstances in which a personal data breach is likely to result in ~~a high risk~~**an "impactful risk" ["relevant risk"/"increased risk"]** to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches. ***The alignment of notification thresholds should not affect the controller's obligation to carry out an individual risk assessment and to maintain complete documentation of personal data breaches in accordance with Article 33(5) and Article 30 of Regulation (EU) 2016/679. The common list of circumstances in which a personal data breach is likely to***

Commission proposal	Drafting suggestions and Comments
	result in a ~~high risk~~*an "impactful risk" ["relevant risk"/"increased risk"] *to the rights and freedom of a natural person should also apply in order to determine when communicating the data breaches to the data subject, in accordance with Article 34. AT (Comments): • AT **remains sceptical** towards raising the threshold for data breach notifications to the supervisory authority. • A possible compromise could be to use a threshold between "risk" and "high risk", such as "impactful risk", "relevant risk", "increased risk" or similar. FI (Comments): FI can support this recital text. SE (Comments): Sweden supports the proposal to allow for the Commission to adopt implementing acts in this regard in accordance with the comitology procedure set out in Article 93(2). Furthermore, in order to ensure effectiveness in the procedure, Sweden considers that the Commission should be given a margin of discretion and be able to review the proposals made by the board.
(39a) In order to facilitate compliance obligations and the establishment of the contract or other legal act governing the processing by a processor on behalf of the controller, the processor should also be subject to the general obligation of data protection by design and by default under Regulation (EU) 2016/679 to extent it relates to its own obligations under that Regulation. This obligation on the processor does	FR (Comments): **Les autorités françaises peuvent soutenir l'introduction de ce nouveau considérant étendant l'application du principe de protection des données dès la conception et par défaut aux sous-traitants.**

Commission proposal	Drafting suggestions and Comments
not affect level of responsibility and relationship between the controller and processor, nor the principle of accountability or the respective obligation of controller and processor as laid down under Article 28 of Regulation (EU) 2016/679). As such, the controller remains solely responsible of determining the purpose and means of processing and apply related obligations, while the processor should ensure that data protection by design and by default is applied to its processing offer and services.	EE (Drafting suggestions): ~~(39a) In order to facilitate compliance obligations and the establishment of the contract or other legal act governing the processing by a processor on behalf of the controller, the processor should also be subject to the general obligation of data protection by design and by default under Regulation (EU) 2016/679 to extent it relates to its own obligations under that Regulation. This obligation on the processor does not affect level of responsibility and relationship between the controller and processor, nor the principle of accountability or the respective obligation of controller and processor as laid down under Article 28 of Regulation (EU) 2016/679). As such, the controller remains solely responsible of determining the purpose and means of processing and apply related obligations, while the processor should ensure that data protection by design and by default is applied to its processing offer and services.~~ EE (Comments): By extending the principles of data protection by design and by default directly to processors as well, it blurs the controller's responsibility under Article 5(2) GDPR. In addition, if Article 28 still provides that the controller determines what the processor must do and how, and the processor acts accordingly, then the purpose of this amendment is not clear. Recital 39a states with regard to processors: "to the extent of its own obligations" — we kindly ask to specify what exactly does this mean in light of the fact that the processor's obligations stem from the contract, while the controller determines the purposes and means of processing? DK (Comments):

Commission proposal	Drafting suggestions and Comments
	DK: regarding the new recital 39a and and the proposed article 25, Denmark understands that it shifts the responsibility for compliance with relevant parts of the GDPR from the controller to the processor. In that case, Denmark can support the provision. However, Denmark cannot support the provision if it merely imposes a burden on the processor that is not offset by a reduction in the burden on the controller. AT (Drafting suggestions): (39a) In order to facilitate compliance obligations and the establishment of the contract or other legal act governing the processing by a processor on behalf of the controller, the processor should also be subject to the general obligation of data protection by design and by default under Regulation (EU) 2016/679 to extent it relates to ~~its~~ **his** own obligations under that Regulation. This obligation ~~**on the processor**~~ does not affect **the** level of responsibility ~~**and**~~ **or the** relationship between the controller and processor, nor **does it affect** the principle of accountability or the respective obligation of **the** controller and **the** processor as laid down under Article 28 of Regulation (EU) 2016/679). ~~**As such**~~**Accordingly**, the controller remains solely responsible ~~**of**~~ **for** determining the purpose and means of processing and ~~**apply**~~ **for complying with** related obligations, while the processor should ensure that data protection by design and by default is applied to its processing **offers** and services. AT (Comments): AT can **support** the addition of Recital 39a but proposes that the wording should be revised. FI (Comments):

Commission proposal	Drafting suggestions and Comments
	Concerning Article 25 GDPR [Art. 3(7a) Digiomnibus] and this recital, FI has reservations to add processors in the Article without a proper assessment but understand that processors should also bear the responsibility especially in situations where SMEs use processors that provide services with "take it or leave it" conditions. However, this is not a redline. CZ (Drafting suggestions): **(39a) In order to facilitate compliance obligations and the establishment of the contract or other legal act governing the processing by a processor on behalf of the controller, the processor should also be subject to the general obligation of data protection by design and by default under Regulation (EU) 2016/679 to extent it relates to its own obligations under that Regulation. This obligation on the processor does not affect level of responsibility and relationship between the controller and processor, nor the principle of accountability or the respective obligation of controller and processor as laid down under Article 28 of Regulation (EU) 2016/679). As such, the controller remains solely responsible of determining the purpose and means of processing and apply related obligations, while the processor should ensure that data protection by design and by default is applied to its offered means and services to carry out processing. When preparing and carrying out the processing of personal data on behalf of a controller, the processor is subject to instructions by controller ~~offer and services~~.** CZ (Comments): In the spirit of compromise, CZ believes that more should be said about relationship between the responsibilities of the controller and processor in line with Article 28. Otherwise, situations where controller and processor have divergent positions on data protection by default and design would not

Commission proposal	Drafting suggestions and Comments
	have a solution. Processor should be responsible at most for its offer to carry out processing, not for the final modalities of processing that must remain in the responsibility of controller (unless Art. 28 is changed as well). SE (Comments): Sweden welcomes the clarification as regards the relationship between the processor and controller. Nevertheless, the wording of the proposed Article 25 does necessarily reflect this division of responsibility and could risk to be interpreted otherwise.
(40) Article 35 of that Regulation (EU) 2016/679 requires controllers to conduct a data protection impact assessment where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. The supervisory authorities established pursuant to that Regulation are required to establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. In addition, the Regulation provides that supervisory authorities may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. In order to effectively contribute to the aim of convergence of the economies and to effectively ensure free flow of personal data between Member States, increase legal certainty, facilitate compliance by controllers and ensure a harmonised interpretation of the notion of a high risk to the rights and freedoms of data subjects, a single list of processing operations should be provided at EU level, to replace the existing national lists. In addition, the publication of a list of the type of processing operations for which no data protection impact assessment is required, which is currently optional, should be made mandatory. The lists of processing operations should be ~~prepared~~**established and made public** by the Board~~ and adopted by the Commission as an implementing act~~**. In establishing the lists, due account should be taken of the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons**. In	NL (Drafting suggestions): (40) Article 35 of that Regulation (EU) 2016/679 requires controllers to conduct a data protection impact assessment where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. The supervisory authorities established pursuant to that Regulation are required to establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. In addition, the Regulation provides that supervisory authorities may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. In order to effectively contribute to the aim of convergence of the economies and to effectively ensure free flow of personal data between Member States, increase legal certainty, facilitate compliance by controllers and ensure a harmonised interpretation of the notion of a high risk to the rights and freedoms of data subjects, a single list of processing operations should be provided at EU level, to replace the existing national lists. In addition, the publication of a list of the type of processing operations for which no data protection impact assessment is required, which is currently optional, should be made mandatory. The lists of processing operations should be established and made public by the Board. In establishing the lists,

Commission proposal	Drafting suggestions and Comments
order to facilitate compliance by controllers, the Board should also ~~prepare~~**establish and make public** a common template and a common methodology for conducting data protection impact assessments~~, to be adopted by the Commission as an implementing act. The Commission should take due account of the proposals prepared by the Board and review them, as necessary, prior to adoption~~. In order to take account of technological developments, the lists and the common template and methodology should be reviewed at least every three years and updated where necessary. **The Commission may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates where necessary.**	due account should be taken of the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. In order to facilitate compliance by controllers, the Board should also establish and make public a common template and a common methodology for conducting data protection impact assessments. In order to take account of technological developments, the lists and the common template and methodology should be reviewed at least every three years and updated where necessary. ~~**The Commission may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates where necessary.**~~ NL (Comments): NL refers to its amendment on Article 35(6a) and 35(6b). EE (Drafting suggestions): (40) Article 35 of that Regulation (EU) 2016/679 requires controllers to conduct a data protection impact assessment where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. The supervisory authorities established pursuant to that Regulation are required to establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. In addition, the Regulation provides that supervisory authorities may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. In order to effectively contribute to the aim of convergence of the economies and to effectively ensure free flow of personal data between Member States, increase legal certainty, facilitate compliance by controllers and ensure a harmonised interpretation of the notion of a high risk to the rights and freedoms of data subjects, a single list of processing operations should be provided at EU level, to replace the existing national lists. In

Commission proposal	Drafting suggestions and Comments
	addition, the publication of a list of the type of processing operations for which no data protection impact assessment is required, which is currently optional, should be made mandatory. The lists of processing operations should be ~~prepared~~established and made public by the Board ~~and adopted by the Commission as an implementing act~~. In establishing the lists, due account should be taken of the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. In order to facilitate compliance by controllers, the Board should also ~~prepare~~establish and make public a common template and a common methodology for conducting data protection impact assessments~~, to be adopted by the Commission as an implementing act. The Commission should take due account of the proposals prepared by the Board and review them, as necessary, prior to adoption~~. In order to take account of technological developments, the lists and the common template and methodology should be reviewed at least every three years and updated where necessary. ~~**The Commission may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates where necessary.**~~ EE (Comments): While we acknowledge the effort to provide a solution to the situation that the list adopted by EDPB might be challenged in the ECJ, we would like to avoid the diminishing of EDPB's autonomy. For this reason, we suggest removing the clauses that permit the Commission to adopt implementing acts FI (Comments): FI can support this recital text.
(40a) In order to ensure consistency of interpretation of this Regulation (EU) 2016/679, it is important that national supervisory authorities ensure that the adoption of guidelines, recommendations and best	LU (Comments):

Commission proposal	Drafting suggestions and Comments
practices at national level on matters already covered by guidelines adopted by the Board, is consistent and does not contradict those issued by the Board, including by updating national relevant guidelines, recommendations and best practices when necessary. It is also important that national supervisory authorities and the Board duly consider matters of consistent application of this Regulation, including when such matters are identified and brought to their attention by controllers or other relevant stakeholders.	We welcome the fact that this point has been redrafted and addressed in a recital, which we consider more suitable. FR (Comments): **Les autorités françaises sont ouvertes à la proposition de la Présidence d'intégrer les éléments en considérants. Il est en effet essentiel que les autorités nationales de protection des données, de la même manière que le CEPD accroissent significativement leurs efforts pour plus de cohérence dans l'application du RGPD. Ce message doit donc figurer dans les amendements apportés par l'omnibus.** **Toutefois, elles soulignent l'importance que figurent également dans l'omnibus numérique des mesures concrètes à destination des opérateurs économiques tendant à l'homogénéisation de l'interprétation du RGPD au sein du marché intérieur. A ce titre, les autorités françaises rappellent qu'elles ont proposé la création d'un mécanisme permettant aux opérateurs de solliciter l'adoption d'un avis par le CEPD à l'article 64 lorsqu'ils constatent des divergences d'interprétation impactant leurs activités transfrontalières. Ce dispositif répondrait directement aux besoins remontés par les acteurs économiques tout en renforçant la cohérence globale du cadre réglementaire. Les autorités françaises sont attachées à l'intégration dans la partie opérative du texte d'une disposition à destination des opérateurs permettant une application plus cohérente du RGPD. Cette proposition, en synergie avec le nouveau considérant 40a, apporterait une réponse équilibrée aux besoins des opérateurs sans compromettre le haut niveau de protection des données du RGPD. Les autorités françaises estiment que l'absence d'intégration de ses propositions à l'article 64 affaiblirait la portée globale du dispositif.** EE (Comments): Estonia supports the amendment. AT

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): (40a) In order to ensure ~~**consistency of**~~ **the consistent** interpretation of this Regulation, ~~**(EU) 2016/679, it is important that**~~ national supervisory authorities **should** ensure that the ~~**adoption of**~~ guidelines, recommendations and best practices **adopted** at **the** national level on matters **that are** already covered by guidelines adopted by the Board, ~~**is**~~ **are** consistent ~~**and does not contradict**~~ **with** those issued by the Board~~**.,**~~ **This** ~~**including by**~~ **includes** updating national relevant guidelines, recommendations and best practices when necessary. ~~**It is also important that**~~ **Moreover**, national supervisory authorities and the Board **should** duly consider matters of consistent application of this Regulation, including when such matters are identified and brought to their attention by controllers or other relevant stakeholders. AT (Comments): AT can support the addition of Recital 40a but emphasises that the independence of supervisory authorities must be preserved. Furthermore, AT proposes that the wording should be revised. MT (Comments): We agree with the proposed recital 40a which solely aims to highlight the need to ensure consistency of interpretation of the GDPR through the adoption of consistent guidelines by national supervisory authorities with those adopted by the EDPB, without mandating actions on behalf of national supervisory authorities as previously proposed in Article 3(11)(aa) of the Proposal. FI (Drafting suggestions): (40a) In order to ensure consistency of interpretation of this Regulation (EU) 2016/679, it is important that national supervisory authorities ensure

Commission proposal	Drafting suggestions and Comments
	that the adoption of guidelines, recommendations and best practices at national level on matters already covered by guidelines adopted by the Board, is consistent and does not contradict those issued by the Board, including by updating national relevant guidelines, recommendations and best practices when necessary. It is also important that national supervisory authorities and the Board duly consider matters of consistent application of this Regulation, including when such matters are identified and brought to their attention by controllers or other relevant stakeholders. **National supervisory authorities shall refrain from adopting guidelines, recommendations and best practices on matters already covered by guidelines, recommendations and best practices issued by the Board and, where necessary, shall update or repeal their national documentation adopted prior to guidelines, recommendations and best practices adopted by the Board in order to ensure consistency of interpretation of this Regulation.** FI (Comments): FI can support recital 40a concerning the consistency of interpretation of the GDPR and the aim to ensure uniform guidelines from data protection authorities. It is important that when the EDPB has given guidance, national data protection authorities should delete or amend their guidance appropriately. FI would have also preferred clarifying this in Article 57 of the GDPR and prefers the previous version, but as a compromise, FI can support a recital as well. FI proposes that the recital would be more specific to ensure that national DPAs' guidelines are deleted or amended, if not in line with the EDPB guidance. See proposal underlined and bolded. BE

Commission proposal	Drafting suggestions and Comments
	(Comments): We preferred the harmonisation of article 57 rather than the recital in 40a. Preference to keep it in the operative text. SK (Comments): **SK:** We support this recital. SE (Comments): SE welcomes that the Presidency's response to the concerns raised about the previous suggested addition to article 57. However, SE suggests an approach where the emphasis is placed on the importance of consistent and uniform application, rather than on the guidelines adopted by the Board. In its current form, the proposed recital could be interpreted as implying that such guidelines are de facto binding for national supervisory authorities, thereby raising questions about their legal nature.
(41) Regulation (EU) 2018/1725 of the European Parliament and of the Council[6] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. ~~Directive (EU) 2016/680 of the European Parliament and of the Council[7] applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.~~ Regulation (EU) 2018/1725 ~~and Directive (EU) 2016/680~~ should be brough into alignment with the amendments to Regulation (EU) 2016/679 introduced by this Regulation. 6 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision	

Commission proposal	Drafting suggestions and Comments
No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj). 7 ~~Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).~~	
(42) As clarified in recital 5 of Regulation (EU) 2018/1725, whenever the provisions of Regulation (EU) 2018/1725 follow the same principles as the provisions of Regulation (EU) 2016/679, those two sets of provisions should, under the case law of the Court of Justice of the European Union, be interpreted homogeneously. The scheme of Regulation (EU) 2018/1725 should be understood as equivalent to the scheme of Regulation (EU) 2016/679. Therefore, this Regulation also amends the provisions of Regulation (EU) 2018/1725 that are concerned by the amendments of Regulation (EU) 2016/679, insofar as the latter amendments are also relevant in the context of the processing of personal data by the Union institutions, bodies, offices and agencies.	FI (Comments): FI can support this recital text.
~~(43) In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Directive (EU) 2016/680 and any other Union legal act applicable to such processing of personal data should follow after the adoption of this regulation, in order to allow for their application as close as possible to the entry into application of the amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.~~	
(43a) Directive 2002/58/EC on privacy and electronic communications ('ePrivacy Directive'), last revised in 2009, provides a framework for the	IT (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
protection of the right to privacy, including the confidentiality of communications. It also specifies Regulation (EU) 2016/679 in relation to processing of personal data in the context of electronic communication services. It protects the privacy and the integrity of subscriber's or user's terminal equipment used for such communications.	*It protects the privacy and integrity of the terminal equipment used by users or subscribers for such communications,* ***provided that the legal identity of the user or subscriber is known to the controller.*** IT (Comments): It is proposed to specify that the ePrivacy Directive applies to users as they are actually identified. Otherwise, any distinction between anonymous and identified users would be lost. The proposal therefore avoids possible interpretations in this sense. The text should be amended as follows:
(44) The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment and the subsequent processing of such data should be regulated under a single legal framework, namely Regulation (EU) 2016/679, where the subscriber of the electronic communications service or the user of the terminal equipment is a natural person. The amendments ~~presented in this Regulation~~**to this Directive should** continue to offer the highest levels of protection for personal data, while simplifying the experiences of data subjects in exerting their rights and expressing their choices online. The amendments concern in particular storage of information in that equipment, accessing or otherwise collecting information from that equipment that entails the processing of personal data through cookies or similar technologies to gain information from the terminal equipment. ~~The relevant rules should also apply regardless of whether the terminal equipment is owned by the natural person or by another legal or natural person.~~	NL (Comments): The reference in the first sentence to Regulation (EU) 2016/679 would not be in line with the rest of the compromise proposal. FR (Drafting suggestions): The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment and the subsequent processing of such data should be regulated under a single legal framework, namely ***Directive 2002/58/EC on privacy and electronic communications***, where the subscriber of the electronic communications service or the user of the terminal equipment is a natural person. The amendments ~~presented in this Regulation~~**to** this Directive should continue to offer the highest levels of protection for personal data, while simplifying the experiences of data subjects in exerting their rights and expressing their choices online. The amendments concern in particular storage of information in that equipment, accessing or otherwise collecting information from that equipment that entails the processing of personal data through cookies or similar technologies to gain information from the terminal equipment. ~~The relevant~~

Commission proposal	Drafting suggestions and Comments
	~~rules should also apply regardless of whether the terminal equipment is owned by the natural person or by another legal or natural person.~~ FR (Comments): Editorial correction to emphasize that the legal framework for cookies is clearly defined by the ePrivacy Directive. MT (Drafting suggestions): (44) The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment and the subsequent processing of such data should be regulated under a single legal framework, namely **Directive 2002/58/EC** ~~**Regulation (EU) 2016/679, where the subscriber of the electronic communications service or the user of the terminal equipment is a natural person**~~. The amendments ~~presented in this Regulation~~***to this Directive should*** continue to offer the highest levels of protection for personal data, while simplifying the experiences of data subjects in exerting their rights and expressing their choices online. The amendments concern in particular storage of information in that equipment, accessing or otherwise collecting information from that equipment that entails the processing of personal data through cookies or similar technologies to gain information from the terminal equipment. ~~The relevant rules should also apply regardless of whether the terminal equipment is owned by the natural person or by another legal or natural person.~~ MT (Comments): We understand that the Presidency's approach is to maintain the current single legal framework (which we support) when it comes to the storing of information, or gaining of access to information already stored in the

Commission proposal	Drafting suggestions and Comments
	terminal equipment of a natural person by amending Article 5(3) of the ePrivacy Directive. However, we note that recital 44 still refers to "*Regulation (EU) 2016/679*" instead of "*Directive 2002/58/EC*". LV (Drafting suggestions): "The amendments presented in this Regulation **to ~~this~~ Directive 2002/58/EC should** continue to offer the highest levels of protection for personal data, while simplifying the experiences of data subjects in exerting their rights and expressing their choices online."
The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment should continue to be allowed only on the basis of consent. ~~Similar to the approach in Directive 2002/58/EC, this requirement should not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, when that is based on Union or Member State law within the meaning of Article 6 of Regulation (EU) 2016/679 and if it fulfils all conditions of lawfulness laid down in that provision, and is done for the objectives laid down in Article 23(1) of Regulation (EU) 2016/679.~~	IT (Drafting suggestions): *The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment and the subsequent processing of such data should be regulated under a single legal framework, namely Regulation (EU) 2016/679, where the subscriber of the electronic communications service or the user of the terminal equipment is a natural person* ***whose legal identity is known to the data controller.*** IT (Comments): In accordance with what was proposed for Recital 43, the first paragraph should be modified as follows: see second column
With a view to reducing the compliance burden and providing legal clarity ~~to controllers~~, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by ~~the data subject~~**a subscriber or user**, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a	NL (Drafting suggestions): With a view to reducing the compliance burden and providing legal clarity, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by a subscriber or user, it is necessary to define a

Commission proposal	Drafting suggestions and Comments
terminal equipment, and subsequent processing that is necessary for those purposes, ~~this Regulation~~**the Directive** should therefore provide that ~~the~~**such** processing is lawful~~. The~~**, including when being carried out jointly with or on the behalf of a** controller~~, such as~~**. For example,** a media service provider, may mandate a ~~processor~~**third party**, such as a market research company, to carry out **such processing.** **Creating aggregated information about the usage of an online service to measure the audience of such a service where it is carried out by the controller of that online service solely for its own use, or by a processor acting jointly with or on behalf of this provider, also referred to as 'audience measurement', means**~~the~~ processing **to obtain insight into the performance and use of the online service in an instantly anonymised, aggregated and general manner. This includes the performance of audience measurement as defined in Regulation (EU) 2024/1083. The aggregated information should not relate to a specific data subject and should therefore be anonymous aggregated information. The data collected should not be further processed for another purpose, combined with data from other services from the provider of the online service or from a third party, such as analytics information from other websites or apps, or shared with third parties.** **Maintaining or restoring the security of a service provided by an information society service provider and requested by the subscriber or user, or the terminal equipment used for the provision of such service, should only be allowed without consent to the extent that the security updates are strictly necessary, proportionate, discretely packaged and do not in any way change the functionality of the software on the terminal equipment, including the interaction with other software or settings chosen by the subscriber or user, the subscriber or user is informed in advance each time an update is being installed, and the subscriber or user has the possibility to turn off the automatic installation of these updates**~~on its behalf~~.	limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment, and subsequent processing that is **strictly** necessary for those purposes, the Directive should therefore provide that such processing is lawful, including when being carried out jointly with or on the behalf of a controller. For example, a media service provider, may mandate a third party, such as a market research company, to carry out such processing. Creating aggregated information about the usage of an online service to measure the audience of such a service where it is carried out by the controller of that online service solely for its own use, or by a processor acting jointly with or on behalf of this provider, also referred to as 'audience measurement', means processing to obtain insight into the performance and use of the online service in an instantly anonymised, aggregated and general manner. This includes the performance of audience measurement as defined in Regulation (EU) 2024/1083. The aggregated information should not relate to a specific data subject and should therefore be anonymous aggregated information. The data collected should not be further processed for another purpose, combined with data from other services from the provider of the online service or from a third party, such as analytics information from other websites or apps, or shared with third parties. Maintaining or restoring the security of a service provided by an information society service provider and requested by the subscriber or user, or the terminal equipment used for the provision of such service, should only be allowed without consent to the extent that the security updates are strictly necessary, proportionate, discretely packaged and do not in any way change the functionality of the software on the terminal equipment, including the interaction with other software or settings chosen by the subscriber or user, the subscriber or user is informed in advance each time an update is being installed, and the subscriber or user has the possibility to turn off the automatic installation of these updates.

Commission proposal	Drafting suggestions and Comments
	NL (Comments):

Commission proposal	Drafting suggestions and Comments
	  Currently, the newly added fraud prevention purpose within the security exception in the proposed article 5(3)(d) eprivacy-directive does not contain any delineation. The corresponding recital text here is still limited to the performance of essential security updates. The unlimited inclusion of any and all fraud prevention measures makes the security exception too broad and creates the risk of enabling various data processing applications that may be unintended or undesirable. In this broad formulation, and in the absence of an explanation of the necessity and meaning, we therefore suggest removing the new addition in the proposed article 5(3)(d) eprivacy-directive. If member states nevertheless want to proceed with a reference to fraud prevention, strict delineation must be included, as well as an explanation in this recital. We make a study reservation for the review of such delineation and explanation.

Commission proposal	Drafting suggestions and Comments
	IT (Drafting suggestions): With a view to reducing the compliance burden and providing legal clarity, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by a subscriber or user, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, the Directive should therefore provide that such processing is lawful, including when being carried out jointly with or on the behalf of a controller, such as. For example, a media service provider, may mandate a third party, such as a market research company, to carry out such processing. Creating ~~aggregated~~ information about the usage of an online service to measure the audience of such a service where it is carried out by the controller of that online service solely for its own use, ~~or~~ by a processor acting jointly with or on behalf of this provider, or by an entitled and independent third party in accordance to Article 24 of Regulation (EU) 2024/1083, also referred to as 'audience measurement', means ~~the~~ processing such data and information to obtain insight into the performance and use of the online service in an instantly anonymised, aggregated and general manner. This includes for instance when it is performed by an entitled and independent third party acting as **independent** data controller jointly authorized by advertisers and publishers, solely for the measurement of the overall market performance. Independent third parties acting on behalf of the media industry, such as Joint Industry Committees, play a critical role in ensuring transparency, comparability, and credibility of audience information across the market ~~the performance~~ of audience measurement as defined in Regulation (EU) 2024/1083. The aggregated information should not relate to a specific data subject and should therefore be anonymous aggregated

Commission proposal	Drafting suggestions and Comments
	information. The data collected should not be further processed for another purpose, combined with data from other services from the provider of the online service or from a third party, such as analytics information from other websites or apps, or shared with third parties. Maintaining or restoring the security of a service provided by an information society service provider and requested by the subscriber or user, or the terminal equipment used for the provision of such service, should only be allowed without consent to the extent that the security updates are strictly necessary, proportionate, discretely packaged and do not in any way change the functionality of the software on the terminal equipment, including the interaction with other software or settings chosen by the subscriber or user, the subscriber or user is informed in advance each time an update is being installed, and the subscriber or user has the possibility to turn off the automatic installation of these updates on its behalf. IT (Comments): The proposed amendment, in line with what has already been highlighted in the comments already circulated, aims to maintain and ensure the role of Joint Industry Committees in audience measurement, in full compliance with the provisions of the EMFA. Furthermore, in the proposed amendment, we have clarified the situation of JICs that operate independently of the online service and therefore do not fall within the category of joint controllers (Article 26 of the GDPR) or data processors (Article 28 of the GDPR). FR (Drafting suggestions): With a view to reducing the compliance burden and providing legal clarity ~~to controllers~~, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by ~~the data subject~~a subscriber or user, it is necessary to define a limitative list of purposes for which the

Commission proposal	Drafting suggestions and Comments
	processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, ~~this Regulation~~the Directive should therefore provide that ~~the~~such processing is lawful~~. The~~, including when being carried out jointly with or on the behalf of a controller~~, such as~~. For example, a media service provider, may mandate a ~~processor~~third party, such as a market research company, to carry out such processing. ~~Creating aggregated information about the usage of an online service to measure the audience of such a service~~ **Measuring the audience of an online service in order to create anonymous aggregated information about its use** where it is carried out by the ~~controller~~ **provider** of that online service ~~solely for its own use~~, or by a **third party such as a market research company or a Joint Industry Committee** acting jointly with ~~or on behalf of~~ this provider, also referred to as 'audience measurement', means~~the~~ processing to obtain insight into the performance and use of the online service in an instantly anonymised, aggregated and general manner. This includes the performance of audience measurement as defined in Regulation (EU) 2024/1083. ~~The aggregated information should not relate to a specific data subject and should therefore be anonymous aggregated information.~~ **Such processing, which contributes to the sustainability of the media ecosystem as highlighted in Regulation 2024/1083, is subject to strict limitations designed to ensure that the data is not reused for advertising, profiling or other unrelated purposes.** ~~The data collected should not be further processed for another purpose, combined with data from other services from the provider of the online service or from a third party, such as analytics information from other websites or apps, or shared with third parties.~~ Maintaining or restoring the security of a service provided by an information society service provider and requested by the subscriber or user, or the terminal equipment used for the provision of such service, should only be allowed without consent to the extent that the security updates are strictly necessary, proportionate, discretely packaged and do not in any way change

Commission proposal	Drafting suggestions and Comments
	the functionality of the software on the terminal equipment, including the interaction with other software or settings chosen by the subscriber or user, the subscriber or user is informed in advance each time an update is being installed, and the subscriber or user has the possibility to turn off the automatic installation of these updates~~on its behalf~~. ***The measurement of the display and performance of advertising which is made solely on the basis of the immediate content displayed on the user's interface, also referred to as 'contextual advertising', may be lawful without the consent of the user provided that it is not based on any type of profiling, that it is based on a user's current visit to a single web page or based on a single search query and does not involve any retention or link with the user's past or future activity.*** FR (Comments): Modification du considérant afin de tenir compte du rôle des organismes tiers de mesure d'audience et de garantir une réglementation adéquate de leurs activités. Réintroduction de l'exemption pour la publicité contextuelle, soutenue par la position française. DK (Drafting suggestions): With a view to reducing the compliance burden and providing legal clarity ~~to controllers~~, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by ~~the data subject~~**a subscriber or user**, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a

Commission proposal	Drafting suggestions and Comments
	terminal equipment, and subsequent processing that is necessary for those purposes, ~~this Regulation~~**the Directive** should therefore provide that ~~the~~**such** processing is lawful~~. The~~**, including when being carried out jointly with or on the behalf of a** controller~~, such as~~**. For example,** a media service provider, may mandate a ~~processor~~**third party**, such as a market research company, to carry out **such processing.** **Creating aggregated information about the usage of an online service to measure the audience of such a service where it is carried out by the controller of that online service ~~solely for its own use~~, or by a ~~processor~~ third party acting jointly with or on behalf of this provider, also referred to as 'audience measurement', means**~~the~~ processing **to obtain insight into the performance and use of the online service in an ~~instantly anonymised.~~ aggregated and general manner. This includes the performance of audience measurement as defined in Regulation (EU) 2024/1083. The aggregated information should not relate to a specific data subject and should therefore be anonymous aggregated information. The anonymous aggregated information can be shared with third parties, including companies and non-commercial organizations. The data collected should not be further processed for another purpose, combined with data from other services from the provider of the online service or from a third party, such as analytics information from other websites or apps, or shared with third parties.** **Maintaining or restoring the security of a service provided by an information society service provider and requested by the subscriber or user, or the terminal equipment used for the provision of such service, should only be allowed without consent to the extent that the security updates are strictly necessary, proportionate, discretely packaged and do not in any way change the functionality of the software on the terminal equipment, including the interaction with other software or settings chosen by the subscriber or user, the subscriber or user is informed in advance each time an update is being installed, and the subscriber or**

Commission proposal	Drafting suggestions and Comments
	user has the possibility to turn off the automatic installation of these updates~~on its behalf~~. DK (Comments): (44) While we appreciate the new reference to EMFA there are still challenges with the wording regarding audience measurement, which should to a greater extent be aligned how audience measurement is carried out. Specifically, we suggest adjusting the text so that: - It reflects that independent audience measurement is carried by actors that are not only processors but also have some degree of control given that they operate independently, and as per EMFA, impartially. Moreover, we take note that the word "processor" has been replaced with "third party" in the corresponding Article 5(3)(c), why "processor" unquestionably should also be replaced by "third party" in the preamble. - Requirements to "instant anonymization and aggregation" are modified to reflect that audience measurement can involve some degree of preliminary processing before aggregation is carried out. - Removing the requirement regarding "… solely for its own use" to reflect that audience measurement is used broadly by a) other commercial companies than the measured entity and b) non-commercial organizations, e.g. in ensuring adherence to legislation and more. To the same end, introducing a sentence stating, that the anonymous aggregated data can be shared with third parties, while, ensuring clarity that the original data collected corresponding to individual users cannot be shared. LV (Drafting suggestions): […] Creating aggregated information about the usage of an online service to measure the audience of such a service where it is carried out by the controller of that online service solely for its own use, or by a processor **or an independent audience measurement provider** acting jointly with or on

Commission proposal	Drafting suggestions and Comments
	behalf of this provider, also referred to as 'audience measurement', means processing to obtain insight into the performance and use of the online service in an instantly anonymised, aggregated and general manner. This includes the performance of audience measurement as defined in Regulation (EU) 2024/1083. The aggregated information should not relate to a specific data subject and should therefore be anonymous aggregated information. The data collected should not be further processed for another purpose, combined with data from other services from the provider of the online service or from a third party, such as analytics information from other websites or apps, or shared with third parties. [..]" LV (Comments): Latvia very much welcomes the inclusion of the new wording in recital 44, which explicitly clarifies that media service providers can mandate processors and third-party market research companies to conduct audience measurement. This is a very positive step in the right direction. We propose some additions to clarify this more. An alternative wording of the addition we would welcome is "providers of audience measurement systems". The addition of "or an independent audience measurement provider" aims to explicitly highlight that such providers fall within the scope of the exemption. Without this clarification, essential audience-measurement scripts delivered by such providers risk being blocked at browser level before users access the service, effectively undermining the purpose of the exemption. Extending the wording ensures that legitimate, privacy-preserving audience measurement can function in practice while remaining limited to anonymised and aggregated data use. HU (Comments):

Commission proposal	Drafting suggestions and Comments
	HU: From a cybersecurity perspective, strictly necessary security updates should be distinguished from functional or commercial software modifications. At the same time, mandating non-deferrable automatic installation would itself create availability and safety risks, since updates are not always sufficiently tested before release and uncontrolled deployment can cause outages, in particular in operational, industrial, medical or other critical environments. We therefore consider that the framework should preserve the operator's ability to test, stage and schedule security updates, including the possibility to defer or switch off automatic installation, while still encouraging prompt remediation. We would also note that the condition that the update "does not in any way change the functionality" may be too absolute, as security remediation may require disabling or removing a vulnerable function, protocol or interface. FI (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~**Creating aggregated information about the usage of an online service to measure the audience of such a service where it is carried out by the controller of that online service solely for its own use, or by a processor acting jointly with or on behalf of this provider, also referred to as 'audience measurement', means the processing to obtain insight into the performance and use of the online service in an instantly anonymised, aggregated and general manner. This includes the performance of audience measurement as defined in Regulation (EU) 2024/1083.**~~ **Audience measurement, as defined in Regulation (EU) 2024/1083, has a direct impact on the allocation and prices of advertising, which represents a key revenue source for the media sector.** The aggregated ~~**information**~~ **results** should not relate to a specific data subject and should therefore be anonymous aggregated information. The data collected should not be further processed for another purpose, ~~**combined with data from other services from the provider of the online service or from a third party, such as analytics information from other websites or apps.**~~ or shared with third parties. FI (Comments): The text should not create a new definition for audience measurement, as this would be against the goal of simplification of digital legislation. The proposed definition of audience measurement in the recital creates one more overlapping and contradictory rule, as audience measurement is already defined in the European Media Freedom Act (EMFA). FI notes that the definition adopted in EMFA cannot be altered in a recital of the digital omnibus.

Commission proposal	Drafting suggestions and Comments
	Article 24(1) of the EMFA mandates that audience measurement must be comparable and verifiable. The proposed specifications in recital 44, particularly the requirement to instantly anonymize data and the prohibition on combining data, would effectively render audience measurement, carried out in compliance with the EMFA, impossible. FI calls for the deletion of requirements that would undermine the conditions necessary to ensure comparability and verifiability, thereby conflicting with article 24(1) of the EMFA. CZ (Drafting suggestions): With a view to reducing the compliance burden and providing legal clarity ~~to controllers~~, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by ~~the data subject~~**a subscriber or user**, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, ~~this Regulation~~**the Directive** should therefore provide that ~~the~~**such** processing is lawful~~. The~~**, including when being carried out jointly with or on the behalf of a** controller~~, such as~~**. For example,** a media service provider, may mandate a ~~processor~~**third party**, such as a market research company, to carry out **such processing.** **Another example is the storing of or access to information in terminal equipment for the purposes of road safety, transport safety, and accident prevention, including the operation, maintenance, and improvement of connected vehicles and mobility systems.** **Creating aggregated information about the usage of an online service to measure the audience of such a service where it is carried out by the controller of that online service solely for its own use, or by a processor acting jointly with or on behalf of this provider, also referred to as**

Commission proposal	Drafting suggestions and Comments
	'audience measurement', means~~the~~ processing **to obtain insight into the performance and use of the online service in an instantly anonymised, aggregated and general manner. This includes the performance of audience measurement as defined in Regulation (EU) 2024/1083. The aggregated information should not relate to a specific data subject and should therefore be anonymous aggregated information. The data collected should not be further processed for another purpose, combined with data from other services from the provider of the online service or from a third party, such as analytics information from other websites or apps, or shared with third parties.** **Maintaining or restoring the security of a service provided by an information society service provider and requested by the subscriber or user, or the terminal equipment used for the provision of such service, should only be allowed without consent to the extent that the security updates are strictly necessary, proportionate, discretely packaged and do not in any way change the functionality of the software on the terminal equipment, including the interaction with other software or settings chosen by the subscriber or user, the subscriber or user is informed in advance each time an update is being installed, and the subscriber or user has the possibility to turn off the automatic installation of these updates~~on its behalf~~.** **The measurement of the display and performance of advertising which is made solely on the basis of the immediate content displayed on the user's interface, also referred to as 'contextual advertising', may be lawful without the consent of the user provided if not based on any type of profiling, in other words based on a user's visit to a single web page or on a single search query, in case it does not involve any data retention or link with the user's past or future activity.** CZ (Comments):

Commission proposal	Drafting suggestions and Comments
	  CZ: The narrow exemptions of Article 5 of the ePrivacy Directive (2002/58/EC) creates significant difficulties for vehicle manufacturers seeking to transfer data out of vehicles; any time the onboard telematics unit or sensors send data externally, it may qualify as "accessing/storing information" under Article 5(3). This challenge is compounded by the fact that a vehicle is rarely used by a single individual; it may be driven by the owner, a family member, an employee, or a short-term renter, with passengers also potentially implicated. In this regard, and given the importance of automotive sector for the EU, including the R&D based in the EU, we suggest adding an example of data processing, which would in our opinion fall under art. 5(3)(b) of the proposal – providing a service explicitly requested by the user. **Reflecting this particular need in the omnibus is a red line for CZ.**

Commission proposal	Drafting suggestions and Comments
	CZ suggests re-instating a new exemption concerning activities that are not based on profiling, i.e. covering low-risk to the rights and freedoms, non-profiling activities that do not involve any retention of personal data beyond the user's active session nor any link to past or future behaviour. We welcomed that the PCY was able to add this exemption to the version discussed earlier, based on a number of MS comments, and regret that this exemption has be removed later. Our suggestion has been inspired by the

Commission proposal	Drafting suggestions and Comments
	EDPB/EDPS joint opinion (point 104) which emphasises the need to create incentives to use less-intrusive forms of online advertising and aimed to make the rules more proportionate, i.e. allowing some forms of targeted advertising, which is crucial for European publishers and service providers. We deem inclusion of this exemption in the EDPB/EDPS joint opinion as an important confirmation that this was a right way forward. Although not a red line, addition of this exemption is of a high priority for Czechia. CZ considers it important that the GDPR allows the Commission to specify through implementing acts, while preserving Member States' control through comitology, other technical modalities than contextual advertising – that are similarly low-risk - to make the provision future proof and to prevent the long-term legislative deadlock phase. The EDPB should be closely involved in the whole process of drafting the acts.
For the ~~subsequent~~**further** processing of personal data for other purpose than those defined in the limitative list, Article 6 and, where relevant, Article 9 of Regulation (EU) 2016/679 should be applied. It is the responsibility of the controller in the light of the principle of accountability to choose the appropriate legal basis for the intended processing. In order to be able to rely on legitimate interest under Article 6(1), point f, of Regulation (EU) 2016/679 as a ground for the ~~subsequent~~**further** processing of personal data, the controller must show that it pursues the controller's or third parties' legitimate interest, the processing is necessary in order to achieve the purpose of that legitimate interest, and the interests or fundamental rights of the data subject do not override the interests pursued by the controller. In this context, controllers should take outmost account of the following elements: whether the data subject is a child; the reasonable expectations of data subject; the	FR (Drafting suggestions): ~~For the subsequent**further** processing of personal data for other purpose than those defined in the limitative list, Article 6 and, where relevant, Article 9 of Regulation (EU) 2016/679 should be applied. It is the responsibility of the controller in the light of the principle of accountability to choose the appropriate legal basis for the intended processing. In order to be able to rely on legitimate interest under Article 6(1), point f, of Regulation (EU) 2016/679 as a ground for the subsequent**further** processing of personal data, the controller must show that it pursues the controller's or third parties' legitimate interest, the processing is necessary in order to achieve the purpose of that legitimate interest, and the interests or fundamental rights of the data~~

Commission proposal	Drafting suggestions and Comments
impact on the individual either because of the scale of data processed or the sensitivity of the data processed; the scale of the processing at issue in the sense that the processing cannot be particularly extensive either because of their amount or the range of categories of data; the processing should be based on data limited to what is necessary and cannot be based on monitoring of large parts of the online activity of the data subjects; and other relevant factors as appropriate. The processing should not give rise to the continuous monitoring of the data subject's private life.	~~subject do not override the interests pursued by the controller. In this context, controllers should take outmost account of the following elements: whether the data subject is a child; the reasonable expectations of data subject; the impact on the individual either because of the scale of data processed or the sensitivity of the data processed; the scale of the processing at issue in the sense that the processing cannot be particularly extensive either because of their amount or the range of categories of data; the processing should be based on data limited to what is necessary and cannot be based on monitoring of large parts of the online activity of the data subjects; and other relevant factors as appropriate. The processing should not give rise to the continuous monitoring of the data subject's private life.~~ FR (Comments): **Les autorités françaises maintiennent leur demande de suppression de ce considérant et de l'article 8a.** Si la référence au RGPD est supprimée, cette partie du considérant n'est, logiquement, plus pertinente.
~~Where the controller cannot rely on legitimate interest as a legal ground for the subsequent processing, the processing should be based on another ground in Article 6(1), in particular on consent in accordance with Articles 6 and 7 of Regulation (EU) 2016/679, provided that all principles of Regulation (EU) 2016/679 are met.~~	
(45) Data subjects that have refused a request for consent are often confronted with a new request to give consent each time they visit the same controller's online service again. This may have detrimental effects to the data subjects which may consent just in order to avoid repeating requests. The controller should therefore be obliged to respect the data subject's choices to refuse a request for consent for at least a certain period. **This obligation is applicable to any controller that accesses or stores personal**	FR (Comments): **Les autorités françaises maintiennent leur demande de suppression de ce considérant et de l'article 8a.**

Commission proposal	Drafting suggestions and Comments
data in the terminal equipment of the data subject, including third party cookie providers.	
(46) Data subjects should have the possibility to rely on automated and machine-readable indications of their choice to consent or refuse a consent request or object to the processing of data. Such means should follow the state of the art. They can be implemented in the settings of a web browser or in the EU Digital Identity Wallet as set out by Regulation (EU) 914/2014, or any other adequate means. Rules set out in this Regulation should support the emergence of market-driven solutions with appropriate interfaces. The controller should be obliged to respect automated and machine-readable indications of data subject's choices once there are available standards. In light of the importance of independent journalism in a democratic society and in order not to undermine the economic basis for that, media service providers should not be obliged to respect the machine-readable indications of data subject's choices. The obligation for providers of web browsers to provide the technical means for data subjects to make choices with respect to the processing should not undermine the possibility for media service providers to request consent by data subjects.	FR (Drafting suggestions): ~~Data subjects should have the possibility to rely on automated and machine-readable indications of their choice to consent or refuse a consent request or object to the processing of data. Such means should follow the state of the art. They can be implemented in the settings of a web browser or in the EU Digital Identity Wallet as set out by Regulation (EU) 914/2014, or any other adequate means. Rules set out in this Regulation should support the emergence of market-driven solutions with appropriate interfaces. The controller should be obliged to respect automated and machine-readable indications of data subject's choices once there are available standards. In light of the importance of independent journalism in a democratic society and in order not to undermine the economic basis for that, media service providers should not be obliged to respect the machine-readable indications of data subject's choices. The obligation for providers of web browsers to provide the technical means for data subjects to make choices with respect to the processing should not undermine the possibility for media service providers to request consent by data subjects.~~ FR (Comments): **Les autorités françaises maintiennent leur demande de suppression de ce considérant et de l'article 8a.** Proposition visant à supprimer le considérant et l'article relatifs à la centralisation du consentement
(46a) Standardisation should play a key role to ensure that technical solutions are available for data subjects to easily set their consent preferences and enable them to make granular and informed decisions.	NL (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
In particular, the standards should enable data subjects to consent, refuse consent and exercise the right to object for direct marketing purposes. The standards should ensure that the conditions for consent under Regulation (EU)2016/679 are fulfilled and enable consent for different purposes. The standards should be prepared in a way that takes into account the operation of businesses in a digital environment and that ensures information is promoted in the digital economy and supports access to content and services on the open web. The standards should ensure that consumer law and competition law requirements are appropriately observed, preventing in particular self-preferencing practices in the provision of the technical solutions that enable setting consent choices.	(46a) Standardisation should play a key role to ensure that technical solutions are available for data subjects to easily set their consent preferences and enable them to make granular and informed decisions. In particular, the standards should enable data subjects to consent, refuse consent**, withdraw consent** and exercise the right to object for direct marketing purposes. The standards should ensure that the conditions for consent under Regulation (EU)2016/679 are fulfilled and enable consent for different purposes. The standards should be prepared in a way that takes into account the operation of businesses in a digital environment and that ensures information is promoted in the digital economy and supports access to content and services on the open web. The standards should ensure that consumer law and competition law requirements are ~~**appropriately observed**~~ **complied with**, preventing in particular self-preferencing practices in the provision of the technical solutions that enable setting consent choices. NL (Comments): To further align this recital with Article 8a(1)(ab) and Article 8a(6) GDPR, NL suggests to include the withdrawal of consent. FR (Comments): **Les autorités françaises demandent à nouveau la suppression de l'article 8a, mais elles peuvent soutenir l'ajout ici en matière d'encouragement au recours à la standardisation pour l'expression du consentement des personnes concernées qui pourrait être conservé même en l'absence de la disposition relative au consentement centralisé.** EE (Comments):

Commission proposal	Drafting suggestions and Comments
	We propose that there should be a deadline for standards. HU (Comments):
	HU: We positively note the additional safeguards and clarifications introduced in Recital 46a regarding machine-readable consent signals, in particular the references to granular and informed consent, consumer protection and competition law considerations, as well as the functioning of the open web. We agree that standardisation should play a central role in the development of machine-readable consent mechanisms and therefore support the Presidency's proposed approach in this regard.
~~(47) Directive 2002/58/EC on privacy and electronic communications 'ePrivacy Directive'), last revised in 2009, provides a framework for the protection of the right to privacy, including the confidentiality of communications. It also specifies Regulation (EU) 2016/679 in relation to processing of personal data in the context of electronic communication services. It protects the privacy and the integrity of user's or subscriber's terminal equipment used for such communications. The current provision of Article 5(3) of Directive 2002/58/EC should remain applicable insofar as the subscriber or user is not a natural person, and the information stored or accessed does not constitute or lead to the processing of personal data.~~	
(48) Article 4 of Directive 2002/58/EC should be repealed. Article 4 of Directive 2002/58/EC sets requirements for providers of publicly available electronic communications services as regards safeguarding the security of their services and notification requirements. Subsequently, Directive (EU) 2022/2555 has set new requirements as regards cybersecurity risk-management measures and incident reporting for those providers. In order to reduce overlapping obligations for entities in the electronic communications sector, Article 4 of Directive 2002/58/EC should be repealed. As regards the security of processing of personal data pursuant to Article 4(1) and (1a) of	

Commission proposal	Drafting suggestions and Comments
this directive and the notification of personal data breaches pursuant to Article 4(3) to (5) of Directive 2002/58/EC this directive, the Regulation (EU) 2016/679 already provide for comprehensive and up-to-date rules. These rules should therefore apply to providers of publicly available electronic communication services and providers of public communications networks, thereby ensuring that one regime applies to the controllers and processors.	
(49) Several horizontal or sectorial Union legal acts require the notification of the same event to different authorities using different technical means and channels. The ~~single-entry~~**establishment by Member States of a national entry** point ~~for incident~~ reporting should allow entities to fulfil reporting obligations under Directive (EU) 2022/2555, Regulation (EU) 2016/679, Regulation (EU) 2022/2554, Regulation (EU) No 910/2014 and Directive (EU) 2022/2557 by submitting notifications to a single interface **at national level**. Furthermore, the single-entry point **established at national level** should give a possibility for entities to retrieve information that they have previously submitted using the single-entry point, thereby helping entities to keep track of their compliance with reporting obligations in connection with specific incidents.	LV (Drafting suggestions): (49) Several horizontal or sectorial Union legal acts require the notification of the same event to different authorities using different technical means and channels. The ~~single-entry~~**establishment by Member States of a national entry** point **for incident** reporting should allow entities to fulfil reporting obligations under Directive (EU) 2022/2555, Regulation (EU) 2016/679, Regulation (EU) 2022/2554, Regulation (EU) No 910/2014 and Directive (EU) 2022/2557 by submitting notifications to a single interface **at national level**. Furthermore, the ~~single-~~entry point **established at national level** should give a possibility for entities to retrieve information that they have previously submitted using the **national** ~~single-~~entry point, thereby helping entities to keep track of their compliance with reporting obligations in connection with specific incidents. LV (Comments): Please clarify why reference reporting of incidents is excluded as it is the main aim of the establishment of national entry points. HU (Comments):

Commission proposal	Drafting suggestions and Comments
	HU still has concerns on the mandatory introduction of the national entry point. Therefore, our scrutiny reservation remains in place until a political decision is taken on the proposal. CZ (Drafting suggestions): Several horizontal or sectorial Union legal acts require the notification of the same event to different authorities using different technical means and channels. The ~~single entry~~**establishment by Member States of a national entry** point ~~for incident~~ reporting **of incidents and related events** should allow entities to fulfil reporting obligations under Directive (EU) 2022/2555, Regulation (EU) 2016/679, Regulation (EU) 2022/2554, Regulation (EU) No 910/2014 and Directive (EU) 2022/2557 by submitting notifications to a single interface **at national level, while allowing for the adaptation of the concrete form and reporting fields of the templates to the specific requirements of the applicable Union legal acts**. Furthermore, the single-entry point **established at national level** should give ~~a~~ **the** possibility for entities to retrieve information that they have previously submitted using the ~~single~~ **national** entry point, thereby helping entities to keep track of their compliance with reporting obligations in connection with specific incidents. CZ (Comments): CZ: CZ appreciates that the proposal offers flexibility enabling Member States to continue using their existing national solutions, including DORA frameworks. In this context, it is important to preserve room for national approaches and avoid creating unnecessary pressure to adapt systems and reporting mechanisms in which Member States have already invested substantially and which are functioning effectively. For CZ it is important that the proposal leaves the decision on the NEP design to the Member States, allowing them to choose the most suitable

Commission proposal	Drafting suggestions and Comments
	approach reflecting country specific conditions building on the interconnection of the already existing systems. RO (Comments): Considering the recitals (50a) and (50b) and the provisions of art. 6 point.1 – adding art. 23a para.(1) point. 2d), art. 6 (3) para.(1) and article 8, we see merits to clarify if only the cyber incidents fall within the scope of the proposal, or all the ICT incidents related or not to a cyber incident. In our opinion, the overlap between ICT incidents and incidents falling within the scope of the GDPR is limited. Consequently, we do not consider this overlap sufficient to justify changing the current competent authority responsible for ICT incident reporting. The proposal to introduce a national single point of entry for the reporting of major ICT incidents does not genuinely reduce the administrative burden, as financial institutions would still be required to prepare and submit separate incident reports under different regulatory frameworks (e.g., DORA, GDPR), each of them with its own taxonomy, templates, and procedures. Furthermore, a major ICT-related incident reported under DORA may require the activation of crisis management procedures. In this context, introducing an additional actor (the national single point of entry) and a new system in the process of receiving incident reports would create significant risk of long delays in the receipt and handling of such incident reports. So, for the time being, we consider that DORA should be excluded from the present Regulation.
(49a) In order to facilitate compliance with the obligation to report incidents and related events, including the identification of the applicable related obligations, ENISA should develop and maintain a single information point for incident reporting. Structured communication channels should be established to ensure that the information available on the single information point is swiftly updated	DK (Comments): DK: The added value of now re-named “incident reporting information point” at EU level remains unclear to us, as ENISA could already create it. AT

Commission proposal	Drafting suggestions and Comments
based on all the relevant and necessary information communicated by Member States.	(Comments): Since the terminology in Art 23a of the compromise text was changed to incident reporting information point it is suggested to reflect this wording also in the recitals. CZ (Drafting suggestions): **(49a) In order to facilitate compliance with the obligation to report incidents and related events, including the identification of the applicable related obligations, ENISA should develop and maintain an ~~single information point for~~ incident reporting information point. That information point should serve as a clearly arranged source of information to support entities in identifying their reporting obligations and to guide them to the appropriate national entry point. Further information on related obligations, especially in terms of cybersecurity risk management, may be added. It should not be used for the submission of notifications of incidents and related events. ~~Structured communication channels should be established to ensure that the information available on the single information point is swiftly updated based on all the relevant and necessary information communicated by Member States.~~** CZ (Comments): CZ: The revision aims to clarify the role of the incident reporting information point as a purely informational and navigational tool. The current wording could be interpreted as leaving room for additional functions, which may create legal uncertainty regarding its scope and relation to national reporting systems. This addition also reflects content of art. 6(1)2d. BE (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	(49a) In order to facilitate compliance with the obligation to report incidents and related events, including the identification of the applicable related obligations, ENISA should develop and maintain a ~~single~~ incident reporting information point for incident reporting. Structured communication channels should be established to ensure that the information available on the single information point is swiftly updated based on all the relevant and necessary information communicated by Member States BE (Comments): Belgium welcomes the simplified language related to the incident reporting information point. Suggestion to align the name of this information point with the name in article 6.
(50) To ensure the security of ~~the single-entry point~~**national entry points in particular and with a view to design interoperable national entry points**, ENISA should ~~take~~**develop guidelines addressing the** appropriate and proportionate technical, operational and organisational measures ~~to manage the risks posed to the security of the single-entry~~**for Member States to develop and maintain their respective national entry** point~~ and the information submitted or disseminated via the single-entry point. When assessing the risk, and the appropriateness and proportionality of those measures, ENISA should take into account the sensitivity of information submitted or disseminated pursuant to the relevant Union legal acts~~. ENISA should consult competent authorities under the relevant Union legal acts when drafting the technical, operational and organisational measures necessary to establish, maintain and securely operate the ~~single-entry~~**national entry** point by making use of existing cooperation groups and networks of Member States established under these acts.	DK (Comments): DK: We note that while aiming to define the term “national entry point”, it also leaves quite some room for interpretation, raising questions as to what extent, the approach to incident reporting will actually be streamlined. HU (Drafting suggestions): (50) To ensure the security of ~~the single-entry point~~**national entry points in particular and with a view to design interoperable national entry points**, ENISA should ~~take~~**develop guidelines addressing the** appropriate and proportionate technical, operational and organisational measures ~~to manage the risks posed to the security of the single-entry~~**for Member States to develop and maintain their respective national entry** point~~ and the information submitted or disseminated via the single-entry point. When assessing the risk, and the appropriateness and proportionality of those measures, ENISA should take into account the sensitivity of information~~

Commission proposal	Drafting suggestions and Comments
	~~submitted or disseminated pursuant to the relevant Union legal acts~~. ENISA should ***establish a cross-sector working group to develop guidelines in*** ~~***consult***~~ ***cooperation with*** competent authorities ***and CSIRTs*** under the relevant Union legal acts when drafting the technical, operational and organisational measures necessary to establish, maintain and securely operate the ~~single-entry~~**national entry** point by making use of existing cooperation groups and networks of Member States established under these acts. HU (Comments): HU: We believe that the development of guidelines should be done with the stronger involvement of MSs, consultation is not enough for this purpose. Thus, we propose that a cross-sector working group be established for the further harmonisation of reporting procedures and templates. This would guarantee a more efficient involvement of the authorities involved. *HU: As national entry points may become concentration points for highly sensitive incident-related information, including vulnerability data, trade secrets, information concerning critical infrastructure and operational data handled by competent authorities, we consider that the ENISA guidelines referred to in this recital should specify minimum technical and organisational security controls. These should include strong authentication, segregation of access between competent authorities, encryption in transit and at rest, audit logging, regular review of access rights, retention limits, as well as availability and overload protection requirements. Since the national entry point may itself become a critical dependency during large-scale incident waves, alternative reporting channels should be tested in advance and properly documented. This point is also reflected in our comment on Article 23b(4).* CZ (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	(50) To ensure the security of ~~the single entry point~~**national entry points** **~~in particular~~ and with a view to design<u>ing</u> interoperable national entry points**, ENISA should ~~take~~**develop <u>non-binding</u> guidelines addressing the** appropriate and proportionate technical, operational and organisational measures ~~to manage the risks posed to the security of the single entry~~**for Member States to develop, ~~and~~ maintain<u>, and securely operate</u> their respective national entry** point ~~and the information submitted or disseminated via the single entry point. When assessing the risk, and the appropriateness and proportionality of those measures, ENISA should take into account the sensitivity of information submitted or disseminated pursuant to the relevant Union legal acts~~. ENISA should consult competent authorities under the relevant Union legal acts when drafting ~~the technical, operational and organisational measures necessary to establish, maintain and securely operate the single entry~~**national entry** ~~point~~ **<u>such guidlines</u>** by making use of existing cooperation groups and networks of Member States established under these acts. RO (Comments): Please consider our comments on recital 49. ES (Comments): See comment on Article 23b(1)
(50a) The term 'national entry point' should be understood as a national infrastructure or arrangement, which may take the form of a digital interface, platform or technical interoperability hub, established and maintained by the Member State, enabling entities to fulfil their incident notification obligations across multiple regulatory frameworks through a single notification at national level which will reach all competent authorities. Member States should retain flexibility to configure such infrastructure or arrangement in accordance with their	NL (Drafting suggestions): **(50a) The term 'national entry point' should be understood as a national infrastructure or arrangement, which may take the form of a <u>web page</u> digital interface, platform or technical interoperability hub, established and maintained by the Member State, <u>supporting</u> ~~enabling~~ entities to fulfil their incident notification obligations across multiple**

Commission proposal	Drafting suggestions and Comments
specific needs, notably their national infrastructures and the allocation of competences among authorities, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information where needed. The creation of the national entry point does not necessarily interfere with the allocation of functions among competent authorities within each national system.	**regulatory frameworks through a single ~~notification~~ entry point at national level which will reach all competent authorities, CSIRT's and/or other designated authorities. Member States should retain flexibility to configure such infrastructure or arrangement in accordance with their specific needs, notably their national infrastructures and the allocation of competences among CSIRT's and competent and/or other designated authorities, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information where needed. The creation of the national entry point does not necessarily interfere with the allocation of functions among competent authorities, CSIRT's and/or other designated authorities within each national system.** NL (Comments): The submission has been jointly developed with ITA and FRA as a common approach. IT (Drafting suggestions): **(50a) The term 'national entry point' should be understood as a national infrastructure or arrangement, which may take the form of a web page, digital interface, platform or technical interoperability hub, established and maintained by the Member State, supporting ~~enabling~~ entities to fulfil their incident notification obligations across multiple regulatory frameworks through a single ~~notification~~ entry point at national level which will reach all competent authorities, CSIRT's and/or other designated authorities. Member States should retain flexibility to configure such infrastructure or arrangement in accordance with their specific needs, notably their national infrastructures and the allocation of competences among CSIRT's and/or other designated authorities, authorities, including by connecting existing systems and**

Commission proposal	Drafting suggestions and Comments
	enabling the sharing, routing or distribution of relevant information where needed. The creation of the national entry point does not necessarily interfere with the allocation of functions among competent authorities, CSIRT's and/or other designated authorities within each national system. IT (Comments): We consider it essential to ensure that national entry points can serve a range of functions, taking into account national arrangements, the level of maturity of each Member State, and the specific characteristics of the national community. In this context, it is important to preserve sufficient flexibility for Member States, so that entry points can effectively act, where appropriate, as information hubs. FR (Drafting suggestions): **(50a) The term 'national entry point' should be understood as a national infrastructure or arrangement, which may take the form of a digital interface, platform or technical interoperability hub, established and maintained by the Member State, supporting ~~enabling~~ entities to fulfil their incident notification obligations across multiple regulatory frameworks through a single ~~notification~~ entry point at national level which will reach all competent authorities, CSIRT's and/or other designated authorities. Member States should retain flexibility to configure such infrastructure or arrangement in accordance with their specific needs, notably their national infrastructures and the allocation of competences among CSIRTS and competent and/or or other designated authorities, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information where needed. The creation of the national entry point does not necessarily interfere with the allocation of functions among competent**

Commission proposal	Drafting suggestions and Comments
	authorities CSIRT's and/or other designated authorities within each national system. FR (Comments): This submission has been jointly developed with Italy and the Netherlands as a common approach. Please see the comments to Article 7. The modifications to recital 50 align with the modifications to Article 7 and aim to ensure more flexibility for Member States to implement national entry point. EE (Comments): First sentence, the end of sentence (words "… competent authorities.") - should this text contain a more general reference to EU legal acts - as it is in the precious recital's second sentence (see the first part)? for example: "... will reach all competent authorities under the relevant Union legal acts." Third sentence, words "competent authorities" - question: at first glance there is no direct need to also include in this part of the sentence also the general reference to EU legal acts - but is it ok, if there is no specification? LV (Comments): It should be specified what is meant by "single notification". Does that entail a single template for all incidents under all legal acts covered by Digital Omnibus that subject must fill in and submit, and NEP will simultaneously distribute it to several supervisory authorities? Will the "single notification" be developed by ENISA as guidelines on harmonization of incident notifications (Article 23c)?

Commission proposal	Drafting suggestions and Comments
	HU (Drafting suggestions): **(50a) The term 'national entry point' should be understood as a *structured, machine-processable* national infrastructure or arrangement, which may take the form of a digital interface, platform or technical interoperability hub, established and maintained by the Member State, enabling entities to fulfil their incident notification obligations across multiple regulatory frameworks through a single notification at national level which will reach all competent authorities. Member States should retain flexibility to configure such infrastructure or arrangement in accordance with their specific needs, notably their national infrastructures and the allocation of competences among authorities, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information where needed. The creation of the national entry point does not necessarily interfere with the allocation of functions among competent authorities within each national system.** HU (Comments): HU: We welcome that the main concept of national entry points is introduced in the text. However, we propose that a structured, machine-processable reporting logic should be the minimum requirement. BE (Drafting suggestions): **The term 'national entry point' should be understood as a national infrastructure or arrangement, which may take the form of a digital interface, platform or technical interoperability hub, established and maintained by the Member State, enabling entities to fulfil their incident**

Commission proposal	Drafting suggestions and Comments
	notification obligations across multiple regulatory frameworks through a single notification at national level which will reach all <u>relevant</u> competent authorities. Member States should retain flexibility to configure such infrastructure or arrangement in accordance with their specific needs, notably their national infrastructures and the allocation of competences among authorities, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information where needed. The creation of the national entry point does not necessarily interfere with the allocation of functions among competent authorities within each national system. BE (Comments): Belgium welcomes the flexibility included in the definition of "National Entry Points" with regards to its' implementation. Addition of "relevant", as not all competent authorities under these acts should be receiving all the incident notifications.
(50b) The development and operation of national entry points may involve important costs for Member States, particularly where national reporting systems need to be built upon existing ones to adapted. It is important that, where applicable and foreseen in the relevant instruments, such activities are financially supported through relevant Union funding instruments, such as the Digital Europe Programme, the European Structural and Investment Funds and other relevant Union funding programmes.	EE (Drafting suggestions): For first sentence two proposals: option a: **The development and operation of national entry points may involve important costs for Member States, particularly where national reporting systems need to be built upon existing ones ~~to adapted~~.** Option b: **The development and operation of national entry points may involve important costs for Member States, particularly where national reporting systems need to be built upon existing ones <u>that need adaptations</u> ~~to adapted~~.** EE (Comments):

Commission proposal	Drafting suggestions and Comments
	Second sentence – we support that such activities are financially supported through relevant Union funding instruments. Regarding the programmes mentioned (the Digital Europe Programme and the European Structural and Investment Funds) - since the new wording mentions that the obligation to use national entry point comes into effect in 30 months after this regulation becomes applicable - then are these Union funding instruments still relevant at the time when this regulation becomes applicable? We propose that there should be a third sentence that has the following idea: "It is also important to ensure that one-off and fixed costs for Member States related to national reporting systems are kept as low as possible." AT (Drafting suggestions): The development and operation of national entry points may involve important costs for Member States, particularly where **new forms of** national reporting systems need to be **set up** ~~built~~ ~~upon~~ **or** existing **systems need** to **be** adapted **and restructured**. It is important that, ~~where applicable and foreseen in the relevant instruments,~~ such activities are financially supported through relevant Union funding instruments, such as the Digital Europe Programme, the European Structural and Investment Funds and other relevant Union funding programmes **to secure financing on a Member State level via contributions of the Union**. AT (Comments): While AT appreciates the considerations regarding possible funding of the NEP, the relevant instruments – as of now – do not foresee financial support for incident reporting structures. Also, the Digital Omnibus proposal at the moment does not introduce any explicit provisions regarding funding. In ATs view the recital as it stands is merely a declaratory policy statement without binding implications. Therefore, it is suggested to include a reference to

Commission proposal	Drafting suggestions and Comments
	financial support/funding in connection to the NEPs (provided that the proposal remains in place) within the legal text. LV (Drafting suggestions): **(50b) The development and operation of national entry points may involve important costs for Member States, particularly where national reporting systems need to be built or ~~upon~~ existing ones need to be adapted. It is important that, where applicable and foreseen in the relevant instruments, such activities are financially supported through relevant Union funding instruments, such as the Digital Europe Programme, the European Structural and Investment Funds and other relevant Union funding programmes.** LV (Comments): Not all Member States have established national entry points therefore financial support by the EU would be significant. HU (Drafting suggestions): **50b) The development and operation of national entry points may involve important costs for Member States, particularly where national reporting systems need to be built upon existing ones to adapted. It is important that~~, where applicable and foreseen in the relevant instruments,~~ such activities are financially supported through relevant Union funding instruments, such as the Digital Europe Programme, the European Structural and Investment Funds and other relevant Union funding programmes.** HU (Comments):

Commission proposal	Drafting suggestions and Comments
	HU: We consider it necessary that if the NEP were made mandatory, a guarantee would be provided that the Member State's obligation is accompanied by an actually accessible EU resource. CZ (Drafting suggestions): **(50b) The development and operation of national entry points may involve ~~important~~ significant costs for Member States, particularly where national reporting systems need to be built, or where already ~~upon~~ existing ones need to be adapted. Further costs might be related to ensuring their cross-border interoperability. It is important that, where applicable and foreseen in the relevant instruments, such activities are financially supported through relevant Union funding instruments, such as the Digital Europe Programme, the European Structural and Investment Funds and other relevant Union funding programmes.** BE (Comments): Belgium strongly supports the possibility to rely on EU funding for the configuration of these National Entry Points. SE (Drafting suggestions): (50b) The development and operation of national entry points may involve ~~important~~ **significant** costs for Member States, particularly where national reporting systems need to be built upon existing ones to adapted. ~~It is important that, where applicable and foreseen in the relevant instruments, s~~Such activities ~~are~~ should be financially supported through relevant Union funding instruments, such as the Digital Europe Programme, the European Structural and Investment Funds and other relevant Union funding programmes. SE

Commission proposal	Drafting suggestions and Comments
	(Comments): Shifting financial burdens to national budgets is not acceptable where expenditures cannot be accommodated within existing financial frameworks. The proposal should must remain budget-neutral for Member States.
(51) ~~Before enabling the~~**It is important to support the further harmonisation of incident** notification ~~of incidents, ENISA should pilot the functioning of the single-entry point which should include a thorough testing of the specificities and requirements for the notifications for the relevant Union legal acts. Based~~**and reporting, including by working** on the ~~results of the piloting, the Commission should assess the proper functioning, reliability, integrity and confidentiality of the single-entry point. The Commission should consult the~~**exchange and interoperability of information regarding incident reporting. For this purpose and in cooperation with the** CSIRTs network ~~and the~~**, the Cooperation Group and** competent authorities under the relevant Union legal acts, ~~by making use of existing cooperation groups and networks of Member States established under these acts, when carrying out the assessment. Where the Commission finds that the single-entry point ensures the proper functioning, reliability, integrity and confidentiality, it should publish a notice to that effect in the Official Journal of the European Union. In case the Commission considers that the proper functioning, reliability, integrity and confidentiality is not ensured,~~ ENISA should ~~take all necessary corrective measures, followed by a reassessment by the Commission~~**develop guidelines to foster the harmonisation of incident notifications**.	EE (Comments): This recital (second sentence) only mentions NIS Cooperation Group and CSIRT Network, but should it also entail other similar groups from other EU Acts – such as: European Data Protection Board (see GDPR Article 68), Oversight Forum (see DORA Regulation Article 32), European Digital Identity Cooperation Group (see eIDAS Regulation Article 46e) and Critical Entities Resilience Group (see CER Directive Article 19)? And in the future, other relevant cooperation groups that are established under current or new EU Acts that might also have in the future the requirement to use national entry points (NEP) - what about those groups? Or should this reference be broader and more future proof? AT (Comments): AT can only emphasise once again that harmonisation seen as a necessary prerequisite and first step towards simplification regarding incident reporting. Only once the incident notification/reporting obligations set out in the various legal acts have been harmonised (in terms of timelines/deadlines as well as information content/common data), will single-entry points – whether established at national or EU-level – actually be able to achieve any kind of simplification and provide added value. Without harmonisation of the reporting obligations across legal acts the NEPs simply cannot provide significant added-value that outweighs the considerable administrative overhead they would cause.

Commission proposal	Drafting suggestions and Comments
	LV (Drafting suggestions): ~~(51) Before enabling the~~**It is important to support the further harmonisation of incident** notification ~~of incidents, ENISA should pilot the functioning of the single-entry point which should include a thorough testing of the specificities and requirements for the notifications for the relevant Union legal acts. Based~~**and reporting, including by working** on the ~~results of the piloting, the Commission should assess the proper functioning, reliability, integrity and confidentiality of the single-entry point. The Commission should consult the~~**exchange and interoperability of information regarding incident reporting. For this purpose and in cooperation with the** CSIRTs network ~~and the~~**, the NIS Cooperation Group and** competent authorities under the relevant Union legal acts, ~~by making use of existing cooperation groups and networks of Member States established under these acts, when carrying out the assessment. Where the Commission finds that the single-entry point ensures the proper functioning, reliability, integrity and confidentiality, it should publish a notice to that effect in the Official Journal of the European Union. In case the Commission considers that the proper functioning, reliability, integrity and confidentiality is not ensured,~~ ENISA should ~~take all necessary corrective measures, followed by a reassessment by the Commission~~**develop guidelines to foster the harmonisation of incident notifications**. CZ (Drafting suggestions): (51) ~~Before enabling the~~**It is important to support the further harmonisation of incident** notification ~~of incidents, ENISA should pilot the functioning of the single-entry point which should include a thorough testing of the specificities and requirements for the notifications for the relevant Union legal acts. Based~~**and reporting, including by working** on the ~~results of the piloting, the Commission should assess the proper functioning,~~

Commission proposal	Drafting suggestions and Comments
	~~reliability, integrity and confidentiality of the single-entry point. The Commission should consult the~~**exchange** ~~**and interoperability**~~ **of information regarding incident reporting. For this purpose and in cooperation with the** CSIRTs network ~~and the~~**, the Cooperation Group and** competent authorities under the relevant Union legal acts, ~~by making use of existing cooperation groups and networks of Member States established under these acts, when carrying out the assessment. Where the Commission finds that the single-entry point ensures the proper functioning, reliability, integrity and confidentiality, it should publish a notice to that effect in the Official Journal of the European Union. In case the Commission considers that the proper functioning, reliability, integrity and confidentiality is not ensured,~~ ENISA should ~~take all necessary corrective measures, followed by a reassessment by the Commission~~**develop guidelines to foster the harmonisation of incident notifications**. BE (Comments): Belgium welcomes the inclusion of other relevant authorities in the consultation process for this report and these guidelines on possible further harmonisation.
~~(52) To ensure the continuity and interoperability with existing national technical solutions that facilitate incident reporting, to the extent feasible, ENISA should take into account such national technical solutions when developing the specifications on the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entry point. Further, ENISA should consider technical protocols and tools such as application programming interfaces and machine-readable standards that enable entities to integrate reporting obligations into business processes, and authorities to connect the single-entry point with their national reporting systems.~~	

Commission proposal	Drafting suggestions and Comments
~~(53) To ensure that the single-entry point enables the relevant entities to submit the type of information and the format required under the relevant Union legal acts, ENISA should consult the Commission and the competent authorities under those acts. Where a Union legal act is not fully harmonized regarding the type of information and the format of notifications, Member States should inform ENISA about their national provisions.~~	
~~(54) Based on Regulation (EU) 2022/2554, the financial sector has been at the forefront in implementing a harmonised, comprehensive and effective framework, including with regard to incident reporting. In order to simplify compliance, it is appropriate to align the incident reporting framework established under Regulation (EU) 2022/2554 with the single-entry point, while ensuring continuity and stability of the existing reporting framework, and considering that the single-entry point would be operational after it has been assessed that it ensures the proper functioning, reliability, integrity and confidentiality. Further, Regulation (EU) 2022/2554 has introduced standardised reporting templates streamlining the content of reports for major ICT-related incidents for the financial sector. The experience gained from the adoption of these templates provides valuable insights and best practices that should be taken into account when specifying the type of information, the format and the procedure of a notification for the purposes of reporting to the single-entry point under Directive (EU) 2022/2555, Directive (EU) 2022/2557 or Regulation (EU) 2016/679, where appropriate. For this purpose, the Commission should take due account of the regulatory technical standards adopted pursuant to Regulation (EU) 2022/2554, which specify the content of the initial notification, as well as the intermediate and final reports, concerning major ICT-related incidents. This approach aims to ensure consistency, promote synergies and reduce administrative burden on entities by minimizing the number of data fields that entities are required to complete, thereby facilitating more efficient and streamlined reporting processes.~~	BE (Comments): What is the reasoning behind the deletion of the DORA best practice in recital 54?

Commission proposal	Drafting suggestions and Comments
(55) Under the relevant Union legal acts, certain incident-specific information is to be shared at a subsequent stage between competent authorities to facilitate effective oversight and coordination. Therefore, the ~~single-entry~~**national entry** point should be designed to accommodate and support the exchange of information at that level for each relevant Union legal act, ensuring that appropriate data flows between authorities are enabled in a secure, timely, and efficient manner, should the Member States decide to make use of this additional feature.	CZ (Drafting suggestions): (55) Under the relevant Union legal acts, certain incident-specific information is to be shared at a subsequent stage between competent authorities to facilitate effective oversight and coordination. Therefore, the ~~single-entry~~**national entry** point should be designed to accommodate and support the exchange of information at that level for each relevant Union legal act, ensuring that appropriate data flows between authorities are enabled in a secure, timely, and efficient manner, **while remaining under the control of Member States**, should the Member States decide to make use of this additional feature.
(56) To ensure that incident reporting is carried out via the ~~single-entry~~**national entry** point Directive (EU) 2022/2555, Regulation (EU) 2016/679, Regulation (EU) 2022/2554, Regulation (EU) 910/2014, and Directive (EU) 2022/2557 should therefore be amended accordingly. The ~~single-entry~~**national entry** point should start being used for the purpose of reporting under those acts within ~~18~~**30** months from the entry into force of this Regulation. ~~When the Commission initiates the mechanisms of the notice delaying the date of application to 24 months from the entry into force of the Regulation, the corresponding provisions of Directive (EU) 2022/2555, Regulation (EU) 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2022/2557 should continue to apply for the purpose of meeting the reporting obligations laid down in the provisions.~~	EE (Drafting suggestions): (56) To ensure that incident reporting is carried out via the ~~single-entry~~**national entry** point Directive (EU) 2022/2555, Regulation (EU) 2016/679, Regulation (EU) 2022/2554, Regulation (EU) 910/2014, and Directive (EU) 2022/2557 should therefore be amended accordingly. The ~~single-entry~~**national entry** point should start being used for the purpose of reporting under those acts within ~~18~~**30** months from the entry into force of this Regulation. Any new amendment to other Union legal acts or new proposals for Union legal acts should establish the date when national entry point should be used for reporting incidents or related events. ~~When the Commission initiates the mechanisms of the notice delaying the date of application to 24 months from the entry into force of the Regulation, the corresponding provisions of Directive (EU) 2022/2555, Regulation (EU) 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2022/2557 should continue to apply for the purpose of meeting the reporting obligations laid down in the provisions.~~ EE

Commission proposal	Drafting suggestions and Comments
	(Comments): We propose an additional new third sentence for the future Union legal acts. LV (Comments): LV sees that it would be valuable to keep reference that deadline for the obligation to report via the national entry point could be extended by 6 months if deemed necessary to keep flexibility as not all Member States have established national entry points that not only will have to be developed but also tested. Moreover, the guidelines by ENISA on technical, operational and organisational measures (Article 23b(4)) for national entry points and on harmonization of incident notifications (Article 23c(3)) should be developed before Regulation enters into force OR the 30 months deadline for the obligation to report via the national entry point should only start after work on these guidelines is concluded. If the development or adaptation of national entry points and work on these guidelines would occur in parallel, that would only create uncertainty for Member States and would hamper the overall process, including meeting the deadline.
(57) In the exceptional event that a technical impossibility prevents the submission of incident notifications using the ~~single entry~~**national entry** point, entities should fulfil their reporting obligations through alternative means. For that purpose, addressees of incident notifications under the relevant Union legal acts should ensure that they can receive such incident notifications through alternative means and should make information about that alternative means publicly available.	EE (Comments): Second sentence, words “should make information about that alternative means publicly available.” - but could the ENISA's "incident reporting information point" be said "source of truth" (in addition to the relevant competent authority's webpage) for such information? AT (Comments):

Commission proposal	Drafting suggestions and Comments
	It seems contradictory to introduce one single NEP for incident reporting that should serve as a replacement for the current reporting systems while requiring the MS to offer alternative means for incident reporting. AT would like a clarification how that alternative means might be structured. Are the MS required to still maintain their current structures in parallel?
(58) The European Data Protection Supervisor ~~was~~**and the European Data Protection Board were** consulted in accordance with Article ~~42(1)~~**42** of Regulation (EU) 2018/1725 of the European Parliament and of the Council[8], and delivered ~~its~~**their joint** opinion on ~~[DATE]. The European Data Protection Board was consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 and delivered an opinion on [DATE]~~**10 February 2026**. 8 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).	
(59) Regulation (EU) 2019/1150 establishes a targeted set of mandatory rules at Union level to ensure a fair, predictable, sustainable and trusted online business environment within the internal market. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 provide a comprehensive regulatory framework for a safe, predictable and trusted online environments for all end-users of online services, and establish a level playing field for businesses in digital markets. In the interest of simplification of Union legislation in the field of online intermediation services and online platforms, and given that the objectives and material provisions of the Platform-to-Business Regulation are largely covered by the Digital Services Act and the Digital Markets Act, **several provisions of** Regulation (EU)	IT (Comments): ITALY welcomes the new version of Recital 59 and Article 10 of the Digital Omnibus (P2B Regulation). In particular, Italy appreciates that the revised Presidency compromise proposal extends the scope of the provisions to be preserved by also including Articles 4 and 11, for which a transitional period had originally been envisaged. Italy supports the Presidency's approach aimed at preserving, for the purposes of legal certainty and maintaining the necessary level of protection

Commission proposal	Drafting suggestions and Comments
~~2019/1050~~**2019/1150** should be ~~repealed~~**deleted**. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 contribute to a fully harmonised regulatory framework for digital services and digital markets, by approximating national measures concerning the requirements for providers of intermediary services and the contestability and fairness of core platforms services provided by gatekeepers. For purposes of legal certainty **and for purposes of keeping the necessary level of protection for business users**, selected definitions in Article 2, ~~the~~ provisions **on terms and conditions in Article 3,** on restrictions and suspensions in Article 4, ~~as well as~~**on ranking in Article 5, and on differentiated treatment in Article 7,** on the internal complaint-handling system in Article 11 ~~of Regulation (EU) 2019/1150 that are cross-referenced by other legal acts, in particular Directive (EU) 2023/2831 on improving working conditions in platform work, and~~**, as well as provisions in** Article 15 ensuring enforcement~~, will temporarily remain in application until the original acts are amended~~ **are maintained**.	for business users, selected definitions in Article 2, the provisions on terms and conditions in Article 3, on restrictions and suspensions in Article 4, on ranking in Article 5, on differentiated treatment in Article 7, on the internal complaint-handling system in Article 11, as well as the provisions in Article 15 ensuring enforcement. In Italy's view, maintaining these provisions in force contributes to safeguarding legal certainty, ensuring regulatory coherence across the Union acquis, and preventing gaps in the protection afforded to business users
(60) Given the technical nature of the amendments proposed in this Regulation and the urgency to deliver on a simplified legal framework, this Regulation should enter into force immediately after its publication in the Official Journal. As appropriate, transitional periods should be afforded for Member States and regulated entities to adjust to the rules.	
(61) The amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 are based on Article 16 TFEU. The amendments to Directive 2002/58/EC are based on Article 16 TFEU and Article 114 TFEU. All other amendments are based on Article 114 TFEU.	

Commission proposal	Drafting suggestions and Comments
HAVE ADOPTED THIS REGULATION:	
(...)	
Article 3 **Amendments to Regulation (EU) 2016/679 (GDPR)**	
Regulation (EU) 2016/679 is amended as follows:	
1. Article 4 is amended as follows:	
~~(a) in point 1, the following sentences are added:~~	EE (Comments): Estonia supports the deletion. CZ (Comments): CZ believes that this Digital Omnibus would be a good opportunity to clarify responsibilities of platforms under GDPR and DSA as regards hosted content and the new judgment C-492/23 Russmedia Digital. It should be clarified that exemptions of liability, to the extent they apply, cover also obligations of platform under GDPR. SK (Comments): **SK:** We support deletion of this proposal.
~~'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that~~	IT (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
~~natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'~~	*(a) in point 1, the following sentences are added:* *'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural* *person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'* IT (Comments): Article 4(a) of the GDPR should be reinstated because it avoids broad interpretations of the concept of identifiability, particularly "chain" interpretations, whereby if, in a data management chain operated by independent entities, one participant is able to identify an individual, then the entire chain is subject to the GDPR, even if it processes anonymous data. Finally, point 38b should be amended to clarify that the notion of scientific research also includes medical research and technological applications: "scientific research" means medical, scientific research as well as their technological applications… EE (Comments): Estonia supports the deletion. AT (Comments): • AT welcomes that the definition of 'personal data' remains unchanged. MT

Commission proposal	Drafting suggestions and Comments
	(Comments): We strongly support the proposed deletion. FI (Comments): FI primarily supports that there are no changes to the definition for personal data. Alternatively, FI can accept possible supplements to the definition of personal data that only codify the CJEU case law and do not change the current level of data protection. This is a redline for FI and FI cannot accept supplements that would go beyond the CJEU case law and would lead to attempts to circumvent the GDPR and would not bring clarity to smaller entities. For instance, FI might be willing to accept the first sentence "Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person" of the COM original proposal, accompanied with clarifying examples in the recital text. SE (Drafting suggestions): ***(xx) Data shall not be considered personal for an entity if that entity is unable to identify the natural person to whom the data relates.*** ***To determine whether the natural person is identifiable, account should be taken of only the means the entity possesses or can obtain and are reasonably likely to be used to identify the natural person directly or indirectly.***

Commission proposal	Drafting suggestions and Comments
	The provision set out in (xx) shall not apply where the entity concerned puts data at the disposal of other persons who possess or can obtain means reasonably likely to be used to identify the data subject. ***In such a case, both the transfer of data by this entity and the subsequent processing of those data by the recipient will be considered as processing of personal data.*** ***The provision set out in (xx) shall not apply if the entity is a processor.*** SE (Comments): SE proposes to include this wording into the main text of the Regulation. We are also in favour of placing this in Article 4.1 as other legal acts refer to this paragraph but we remain flexible to place this provision in a separate article, such as Article 29a. The drafting seeks to clarify the definition of personal data by codifying established case law, while remaining closely aligned with the wording used by the Court of Justice of the European Union. The final sentence, clarifying that the provision does not apply to processors, introduces an additional element that does not flow directly from existing case law. This addition is intended to ensure that the proposal does not extend to situations in which a processor receives pseudonymised personal data from a controller. Including processors could otherwise create a risk of circumvention of the regulatory framework, for example by calling into question the applicability of the security obligations under Article 32, thereby increasing the risk of data breaches.

Commission proposal	Drafting suggestions and Comments
(b) the following points are added:	
'(32) 'terminal equipment' means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC;	FR (Drafting suggestions): ~~**'(32) 'terminal equipment' means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC;**~~ FR (Comments): **Les autorités françaises rappellent leur demande de suppression du nouvel article 8a. Cette définition ne serait mobilisée que pour cet article, il convient donc de la supprimer également.** En ce qui concerne la proposition visant à supprimer le mécanisme de consentement centralisé : ces définitions relatives au traitement des cookies sont destinées à être intégrées dans la directive eprivacy ; leur inclusion dans le RGPD n'est donc pas pertinente.
~~(33) for 'electronic communications networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;~~	EE (Comments): Estonia supports the deletion.
(34) 'web browser' means web browser as defined in Article 2(11) of Regulation (EU) 2022/1925;	FR (Drafting suggestions): ~~**34) 'web browser' means web browser as defined in Article 2(11) of Regulation (EU) 2022/1925;**~~ FR (Comments): **Les autorités françaises rappellent leur demande de suppression du nouvel article 8a. Cette définition ne serait mobilisée que pour cet article, il convient donc de la supprimer également.**

Commission proposal	Drafting suggestions and Comments
(35) 'media service' means a media service as defined in Article 2(1) of Regulation (EU) 2024/1083;	FR (Drafting suggestions): ~~**35) 'media service' means a media service as defined in Article 2(1) of Regulation (EU) 2024/1083;**~~ FR (Comments): **Les autorités françaises rappellent leur demande de suppression du nouvel article 8a. Cette définition ne serait mobilisée que pour cet article, il convient donc de la supprimer également.**
(36) 'media service provider' means a media service provider as defined in Article 2(2) of Regulation (EU) 2024/1083;'	NL (Comments): The NL maintains its study reservation regarding the exception for media service providers in Article 8a(3). FR (Drafting suggestions): ~~**36) 'media service provider' means a media service provider as defined in Article 2(2) of Regulation (EU) 2024/1083;'**~~ FR (Comments): **Les autorités françaises rappellent leur demande de suppression du nouvel article 8a. Cette définition ne serait mobilisée que pour cet article, il convient donc de la supprimer également.**
(37) 'online interface' means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065.'	FR (Comments):

Commission proposal	Drafting suggestions and Comments
	Les autorités françaises rappellent leur demande de suppression du nouvel article 8a. Cette définition ne serait mobilisée que pour cet article, il convient donc de la supprimer également.
(38) ~~"~~"scientific research~~"~~" means any research ~~which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways~~ **conducted in an autonomous and independent manner**,~~ be carried out~~ with the aim of contributing to the growth of ~~society´s~~ **society's** general knowledge and wellbeing**, generating new or complementing existing scientific knowledge, following a methodological and systematic approach consistent with standards of the relevant scientific field, including**~~ and adhere to~~ ethical standards~~ in the relevant research area. This does not exclude that the research may also aim to further a commercial interest~~**, and producing verifiable and transparent results**.'	IT (Drafting suggestions): *"scientific research" means* ***medical, scientific research as well as their technological applications*** FR (Comments): **Si les autorités françaises peuvent accepter, à titre de compromis, le nouveau considérant 28, dont la rédaction provient dans l'ensemble de la version précédente du considérant 29, elles regrettent toutefois que la notion de concours à l'intérêt public de la recherche menée ait disparu de la définition elle-même à l'article 4.** EE (Drafting suggestions): (38) ~~"~~"scientific research~~"~~" means any research ~~which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways~~ conducted in an autonomous and independent manner,~~ be carried out~~ with the aim of contributing to the growth of ~~society´s~~ society's general knowledge and wellbeing, generating new or complementing existing scientific knowledge, following a methodological and systematic approach consistent with standards of the relevant scientific field, including~~ and adhere to~~ ethical standards~~ in the relevant research area. This does not exclude that the research may also aim to further a commercial interest~~, and producing verifiable and transparent results.' **Scientific**

Commission proposal	Drafting suggestions and Comments
	research also means research, which can support innovation, such as technological development and demonstration. EE (Comments): We welcome the introduction of a common definition of 'scientific research' under the GDPR. It is essential that the definition does not hinder or restrict the objective of fostering technological development. We believe that it is not enough just to change the recital, as it must be made clear in the operative part of the text that technological development is also part of scientific research. AT (Comments): • AT **continues to reject** the inclusion of a definition for "scientific research" and sees the risk that pseudo-scientific research could also be included in the compromise proposal. • Instead of attempting to introduce a new definition, reference should be made to existing definitions in sector-specific Union law. • AT remains open to the inclusion of explanations in Recital (29), subject to further examination (see above). In this context we refer to the EDPB Guidelines 1/2026 on processing of personal data for scientific research purposes. • In case a definition is included, AT also has concerns about the draft proposals for Articles 5(1)(b) and 13(5). FI (Comments): FI can support the proposed definition for scientific research as it includes all the necessary elements for scientific research. FI can support the recitals 28 and 32 which are balanced and take into account both the public and private interests.

Commission proposal	Drafting suggestions and Comments
	CZ (Drafting suggestions): (38) "'scientific research"' means any research ~~which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways~~ **conducted** ~~**in an autonomous and independent manner,**~~ ~~be carried out~~ with the aim of contributing to the growth of ~~society´s~~ **society's** general knowledge and wellbeing**, generating new or complementing existing scientific knowledge, following a methodological and systematic approach consistent with standards of the relevant scientific field, including** ~~and adhere to~~ ethical standards ~~in the relevant research area. This does not exclude that the research may also aim to further a commercial interest~~**, and producing verifiable and transparent results**. **This does not exclude that the research may also aim to further a commercial interest.** CZ (Comments): CZ: The phrase "autonomous and independent manner" should be deleted as these terms are very uncertain and are not clarified in a recital 29 (see our comments there). GDPR uses "autonomous manner" only in relation to DPO (recital 97), which is not really a position equivalent to researchers. The last part is proposed as it is already contained in recital 29. SK (Comments): **SK:** We welcome the proposed changes and we see that they also reflect EDPB guidelines on scientific research purposes. PL (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	We propose the following wording: "scientific research" means research conducted in a methodological and systematic manner, consistent with ethical standards of the relevant scientific field, with the aim of generating new or complementing existing knowledge and contributing to scientific understanding and societal wellbeing. PL (Comments): The definition should not be interpreted as excluding legitimate scientific research conducted by private entities, including research and innovation activities carried out outside traditional academic environments. This an important element of the simplification package to support EU competitiveness. We would very much welcome a discussion on CRP on this.
2. Article 5 (1)(b) is replaced by the following:	
'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, **subject to the application of appropriate safeguards** in accordance with Article 89(1), be considered to be compatible with the initial purposes, independent of the conditions of Article 6(4) of this Regulation~~,~~ ('purpose limitation');'	LU (Drafting suggestions): collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, ***subject to the application of appropriate safeguards*** in accordance with Article 89(1), be considered to be compatible with the initial purposes, independent of the conditions of Article 6(4) of this Regulation**, and no legal basis separate from that which allowed the collection of the personal data is required**~~,~~ ('purpose limitation');' LU (Comments):

Commission proposal	Drafting suggestions and Comments
	We suggest to partially include recital (50) of the GDPR in Article 5(1)(b) in order to specify that in case of compatible further processing, no legal basis - separate from that which allowed the collection of the personal data- is required. EE (Comments): Estonia supports the amendments. AT (Comments): • In principle, AT would be open to this proposal. However, in light of the also proposed very broad definition of "scientific research" (see AT comments on Article 4(38) above), AT **cannot support it**. • Extended possibilities for processing of personal data for (pseudo-)scientific research purposes would lead to an increase of the volume of personal data processed for this purpose, which would constitute strong interferences with the rights of the data subject and entail a higher risk of data protection infringements. FI (Comments): FI can support this proposal. CZ (Comments): CZ strongly supports this compromise wording. SI (Comments): We propose that at least a minimum set of "appropriate safeguards" is clearly specified, and that the requirement to comply with the conditions laid down in Article 6(4) is maintained.

Commission proposal	Drafting suggestions and Comments
3. Article 9 is amended as follows:	
(a) in paragraph 2, the following points are added:	BE (Comments): Any additional safeguard on AI processing issue is very much welcomed. To Belgium, the word "manifestly" in article 3(3), 9(2)(k) is critical
'(k) **incidental and residual** processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model **as referred to in Regulation (EU) 2024/1689**, subject to the conditions referred to in paragraph 5.	NL (Drafting suggestions): '~~**(k) incidental and residual processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model as referred to in Regulation (EU) 2024/1689, subject to the conditions referred to in paragraph 5.**~~ NL (Comments): NL remains seriously concerned about the proposed derogation to the prohibition on processing special categories of personal data for "residual" data when training and using AI (Article 9(2)(k) and 9(5) GDPR), presently retained by the presidency in the third compromise proposal. This derogation risks normalising the presence of sensitive data in training, testing, validation, systems and models, which by themselves do not justify the processing of such sensitive data. Operators of AI systems would be allowed to process special categories of personal data if its removal would cause "disproportionate effort". This reverses the protective logic of data protection law and risks creating a perverse incentive: the more data are processed, the easier it becomes to

Commission proposal	Drafting suggestions and Comments
	justify the processing of special categories of personal data. NL fears that this exception - specifically for (generative) AI - lends itself to (very) liberal application in practice. Therefore, NL has repeatedly proposed to delete this exception, as it risks broad misuse. However, if a majority of the Member States supports this exception, NL considers it crucial that the conditions should be strictly limited (see below under Article 9(5) and our comments and suggestions regarding Recital 33). LU (Comments): It is indeed appropriate to further clarify the scope of the new derogation, in line with the suggestion put forward by the EDPB and the EDPS. In this context, the addition of the terms “incidental and residual” to describe the processing of sensitive data appears to be a welcome refinement. Second, we believe that this exception could more generally refer to the existence of measures to safeguard the fundamental rights and the interests of the data subject. This would oblige the controller to put into place measures to protect the fundamental rights and interests of the data subject whilst allowing him/her to identify and use the adequate ones on a case-by-case basis. A more general reference would allow the data controller to use other means which might prove more effective to protect the rights and interest of data subjects AT (Comments): AT can **support** the changes in Article 9(2)k. MT (Comments):

Commission proposal	Drafting suggestions and Comments
	See the comment on recital 33. The term "*operation*" is not defined in the GDPR or the AI Act, and thus, this term should be clarified or possibly changed to "*deployment"*. FI (Comments): FI supports the derogation for AI-processing in Article 9 GDPR. FI can support the proposed text and safeguards. It is important that the derogation applies only to incidental and residual processing of special categories of personal data. CZ (Comments): CZ may accept this wording in the spirit of compromise, even though undefined notions of "incidental" and "residual" are likely to introduce legal uncertainty later. SE (Comments): Regulation (EU) 2024/1689 (AI Act) does not provide a standalone definition of the term "AI model." Instead, the AI Act only defines the more specific concept of a "general-purpose AI model." From Sweden's perspective, the absence of an explicit definition of the term "AI model" is not considered to be problematic. Rather, the term should be seen as reflecting that the scope of the Regulation extends beyond "AI systems". In addition, it is considered that a definition of "AI model" should not be introduced in this legal act, particularly as the term is already widely used and generally well understood in it self. PL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): We maintain our previous suggestion: '(k) incidental and residual processing, which is strictly unintended and unavoidable despite the implementation of appropriate technical and organisational measures, in the context of the development and operation of an AI system (…)' PL (Comments): We acknowledge the inclusion of Recital 33, which provides additional guidance regarding the notion of "incidental and residual processing". However, the operative provision itself remains unchanged. While the recital clarifies that such processing should occur only exceptionally and despite the implementation of safeguards, the legal conditions defining the scope of the derogation remain absent from Article 9(2)(k) itself. As a result, the key concepts triggering the application of the exception continue to rely primarily on interpretative guidance rather than on binding normative language. Given that Article 9 GDPR establishes a prohibition on the processing of special categories of personal data and that any derogation from this prohibition should be interpreted strictly, the substantive limits of the exception should be reflected directly in the operative provision. Reliance solely on recital language may not sufficiently ensure legal certainty, consistent application across Member States, or effective compliance by controllers. We therefore maintain that further clarification within Article 9(2)(k) itself would be beneficial, in particular to ensure that the derogation remains

Commission proposal	Drafting suggestions and Comments
	limited to processing that is genuinely unintended and unavoidable despite the implementation of appropriate safeguards.
(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the **one-to-one** verification is under the sole control of the data subject **and, where applicable, subject to appropriate safeguards to protect the fundamental rights and the interests of the data subject, as laid down in Union law or Member State law, in accordance with paragraph 4 of this Article**.'	NL (Comments): NL thanks the Presidency for the improvements of Article 9(2)(l), which NL supports. LU (Comments): The replacement of an additional authorization under national law with the phrase "subject to appropriate safeguards laid down in Union or member State law" doesn't appear, at this stage, to address our concern of a risk of fragmentation between Member States' legal regimes. EE (Comments): Estonia supports the amendment on Art 9 (2) (l) of the GDPR, that there is a possibility, not obligation to introduce protective measures into national law AT (Comments): AT can **support** the changes in Article 9(2)l. FI (Comments): Concerning the derogation for biometric verification in Article 9 GDPR [Art 3(3)(a) Digiomnibus], FI would have preferred to harmonise this matter in the GDPR, complemented with additional safeguards. FI can show flexibility in this (not a redline), although this proposal does not support the aim to simplify. If majority supports this proposal, FI can accept it.

Commission proposal	Drafting suggestions and Comments
	CZ (Comments): CZ strongly supports this compromise wording. The phrase "where applicable" together with reference to non-obligatory paragraph 4, is **a red line for CZ.** SK (Drafting suggestions): processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the **one-to-one** verification is under the sole control of the data subject ~~**and, where applicable, subject to appropriate safeguards to protect the fundamental rights and the interests of the data subject, as laid down in Union law or Member State law, in accordance with paragraph 4 of this Article**~~ SK (Comments): **SK:** The reference to Article 9(4) is not found in any other exception in Article 9(2). We propose to delete this part. In our view, this does not add any value, as Article 9(4) is only an option for Member States and this text merely repeats it. We are in favour of keeping this text only in recital 37. PL (Comments): We maintain our previous concerns regarding the notion of "sole control" of the data subject. The current wording assumes that the existence of sole control can serve as a sufficiently clear criterion for permitting the processing of biometric data for verification purposes. However, in practice, the degree of control exercised by a data subject over biometric credentials, templates, devices or

Commission proposal	Drafting suggestions and Comments
	verification mechanisms may vary considerably depending on the technological solution used. Without further clarification, there is a risk that the notion of "sole control" could be interpreted differently across Member States and across sectors, leading to divergent implementation of the derogation. This may be particularly relevant in situations involving cloud-based authentication services, identity wallets, delegated credential management solutions or other complex technological environments. We therefore continue to consider it appropriate to clarify in the operative provision that the processing should be strictly limited to what is necessary for verification purposes and should not be used for any other purposes. ES (Comments): **Spain**. We very much welcome including "*where applicable*", please keep it that way. It will be a red line for Spain if *where applicable* would be deleted.
(b) the following paragraph is added:	
'5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid ~~v~~ the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data **that are incidentally and residually involved** in the datasets used for training, testing or validation or in the AI system ~~or AI model~~, the controller shall ~~remove~~ **erase** such data. If ~~removal~~ **erase** of those data **proves to be impossible or** requires **manifestly** disproportionate effort, the controller shall ~~in any event effectively protect~~**,** without undue delay **and in any event, effectively protect** such data from being **further processed or processed for other purposes,** used to produce outputs, ~~from being~~ disclosed or otherwise made available to third parties.	NL (Drafting suggestions): 5. For processing referred to in point (k) of paragraph 2, **this derogation shall apply only where special categories of personal data appear incidentally and unintentionally, where the processing does not rely on such data, and where the controller has implemented** appropriate organisational and technical measures ~~**shall be implemented**~~ to avoid the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data that are incidentally and residually involved in the datasets used for training, testing or validation or in the AI

Commission proposal	Drafting suggestions and Comments
The controller shall establish a process of regular verification and assessment of the effectiveness of the measures implemented and shall comprehensively document those measures and the results of the assessments throughout the life cycle of the AI system.'	system, the controller shall erase such data **without undue delay**. If erasure of those data proves to be **technically** impossible ~~**or requires manifestly disproportionate effort**~~, the controller shall, without undue delay and in any event, effectively protect such data from being further processed or processed for other purposes, used to produce outputs, disclosed or otherwise made available to third parties. The controller shall establish a process of regular verification and assessment of the effectiveness of the measures implemented and shall comprehensively document those measures and the results of the assessments throughout the life cycle of the AI system.' NL (Comments): As noted above, NL considers it crucial that Article 9(5) should be strictly limited: the exception should not be applicable in case of a 'disproportionate effort' to remove the personal data, but should be only be applicable where removal is "technically impossible". Furthermore, the exception should be limited in other ways, for example by defining 'incidental and residual' strictly (that the processing may not rely on the special categories of data). Moreover, the "appropriate organisational and technical measures" have to be specified further, for example in Recital 33, including also the obligation to filter out special categories of personal both during data collection and immediately after data collection (cf. EDPB, Report of the work undertaken by the ChatGPT Taskforce, adopted on 23.05.2024, p 7, §19 and §17). LU (Comments): Paragraph 5 of this provision, which outlines the conditions under which such processing may occur, is still being examined at national level. At this stage, our reflections are focused on:

Commission proposal	Drafting suggestions and Comments
	a) the degree of prescriptiveness of the steps envisaged for controllers, particularly ensuring that the provision remains sufficiently flexible to accommodate the diversity of situations in practice; b) the articulation between this provision and article 4a of the AI Omnibus on processing sensitive data for bias detection. FR (Drafting suggestions): '5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid ~~v~~ the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data **that are incidentally and residually involved** in the datasets used for training, testing or validation or in the AI system ~~or AI model~~, the controller shall ~~remove~~ **erase** such data. If ~~removal~~ **erase** of those data **proves to be impossible or** requires **manifestly** disproportionate effort, the controller shall ~~in any event effectively protect~~**,** without undue delay **and in any event, effectively protect** such data from being **further processed or processed for other purposes,** used to produce outputs, ~~from being~~ disclosed or otherwise made available to third parties. ~~**The controller shall establish a process of regular verification and assessment of the effectiveness of the measures implemented and shall comprehensively document those measures and the results of the assessments throughout the life cycle of the AI system.'**~~ FR (Comments): **Les autorités françaises réitèrent leur demandera de suppression de la dernière phrase du paragraphe afin de ne pas alourdir la charge des responsables de traitement. Elles rappellent que les responsables de traitement doivent déjà être en capacité de démontrer qu'ils respectent les**

Commission proposal	Drafting suggestions and Comments
	obligations qui leurs incombent en vertu du RGPD, ce qui rend cette mention superfétatoire, au-delà des difficultés techniques qu'elle pourrait poser pour les opérateurs, induisant une insécurité juridique qu'il est nécessaire d'éviter. AT (Comments): AT **can support** the changes in Article 9(5). FI (Comments): FI supports the derogation for AI-processing in Article 9 GDPR. FI can support the proposed text and safeguards. It is important that the derogation applies only to incidental and residual processing of special categories of personal data. CZ (Drafting suggestions): '5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid ~~v~~ the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data **that are incidentally and residually involved** in the datasets used for training, testing or validation or in the AI system ~~or AI model~~, the controller shall ~~remove~~ **erase** such data. If ~~removal~~ ~~erase~~ **erasure** of those data **proves to be impossible or** requires ~~manifestly~~ disproportionate effort, the controller shall ~~in any event effectively protect~~**,** without undue delay **and in any event, effectively protect** such data from being ~~further processed or~~ **processed for other purposes,** used to produce outputs, ~~from being~~ disclosed or otherwise made available to third parties. **The controller shall establish a process of regular verification and**

Commission proposal	Drafting suggestions and Comments
	assessment of the effectiveness of the measures implemented and shall comprehensively document those measures and the results of the assessments throughout the life cycle of the AI system.' CZ (Comments): CZ: - "manifestly" should be deleted as it is contrary to GDPR standard of "disproportionate effort" and would create interpretative difficulties and uncertainties. - "Further processing" is distinguished from "processing for other purposes" thus clearly involves situations other than Art. 64) GDPR. In this wording, data are further processed even by storage and other operations under Art. 4(4) GDPR. The provision therefore requires contradictory duties – erasure is required, exception is created for impossible situations while inference or disclosure is prohibited, but storage is precluded as well. Either "further processed" should be deleted or the text should be brought in line with Art. 6(4) or 13(3) or 14(4) GDPR: "further processed for other purposes". PL (Comments): While we support the objective of ensuring safeguards in situations involving incidental processing of special categories of personal data, we remain concerned that paragraph 5 continues to introduce a highly detailed and prescriptive compliance framework. The provision goes beyond establishing substantive safeguards and increasingly regulates how controllers must organise and document their compliance activities throughout the lifecycle of an AI system. In particular, the cumulative obligations relating to prevention measures, deletion

Commission proposal	Drafting suggestions and Comments
	assessments, protection mechanisms, regular verification, effectiveness assessments and comprehensive documentation create a compliance structure that significantly exceeds what is typically required under the GDPR accountability framework. This raises concerns regarding proportionality and regulatory coherence. Articles 5(2), 24 and 25 GDPR already require controllers to implement appropriate organisational and technical measures and to demonstrate compliance. Additional obligations should therefore be carefully assessed to avoid unnecessary duplication and excessive administrative burden. In its current form, paragraph 5 risks discouraging reliance on Article 9(2)(k) even in situations that the provision is specifically intended to address. Further simplification and closer alignment with the existing GDPR accountability framework is needed. While the earlier version raised concerns due to its broad and open-ended character, the current wording risks becoming excessively prescriptive by introducing a highly detailed and cumulative set of operational requirements. In our view, the provision should maintain an appropriate balance between effective safeguards for special categories of personal data and practical implementability. A more balanced approach would better ensure both a high level of data protection and the effective usability of the derogation in situations for which it is intended.
4. In Article 12, paragraph 5 is replaced by the following:	SK (Comments): **SK:** We support this proposal
‘5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or	EE (Comments): Estonia supports the amendment.

Commission proposal	Drafting suggestions and Comments
~~also, for requests under Article 15 because~~ **where an abusive intention on the part of** the data subject ~~abuses the rights conferred by this regulation for purposes other than the protection of their data~~ **submitting those requests can be demonstrated**, the controller may either:	AT (Comments): AT **continues to support** the changes to Article 12(5). FI (Comments): FI can support this proposal. CZ (Drafting suggestions): '5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or **also, for requests under Article 15 because**~~***where an abusive intention on the part of***~~ the data subject **abuses the rights conferred by this regulation for purposes other than the protection of their data**~~***submitting those requests can be demonstrated***~~, the controller may either: CZ (Comments): CZ can accept current text in the spirit of compromise. However, given the excessive and often AI-powered requests to both controllers and DPAs, CZ would welcome using the Commission's original wording. CZ could also support other similar proposals. (Commission's wording should be used not only here but also in Article 57(4) GDPR (see below). CZ is aware of judgment C-416/23 but believes that simplification efforts could offer alternative solution.) PL

Commission proposal	Drafting suggestions and Comments
	(Comments): We maintain our previous position because the wording of the provision has not been changed and the notion of "abusive intention" still remains insufficiently precise and may lead to divergent interpretations and inconsistent application of the provision across Member States, in particular as regards the controller's ability to demonstrate the grounds for concluding that such intention existed on the part of the data subject.
(a) charge a reasonable fee ~~taking into account~~ **proportionate to** the administrative costs of providing the information or communication or taking the action requested; or	EE (Comments): Estonia supports the amendment. FI (Comments): FI can support this proposal.
(b) refuse to act on the request **and inform the data subject of the reasons thereof**.	FI (Comments): FI can support this proposal.
The controller shall bear the burden of demonstrating**, in the light of all the relevant circumstances of the case,** that the request is manifestly unfounded or ~~that there are reasonable grounds to believe that it is~~ excessive.'	EE (Comments): Estonia supports the amendment. FI (Comments): FI can support this proposal. CZ (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	The controller shall bear the burden of demonstrating~~***, in the light of all the relevant circumstances of the case,***~~ that the request is manifestly unfounded or **that there are reasonable grounds to believe that it is** excessive.' CZ (Comments): CZ can accept current text in the spirit of compromise. However, given the excessive and often AI-powered requests to both controllers and DPAs, CZ would strongly support using the Commission's original wording. CZ could also support other similar proposals. PL (Drafting suggestions): Proposal for changes: „The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive or submitted with an abusive intention, based on objective circumstances related to the request or the conduct of the data subject." ES (Comments): **Spain**. We want to add this paragraph: "The exercise of the rights recognized in Articles 15 to 22 shall not be conditional upon the obligation of the interested party to justify his request. However, the total absence of indication on the purpose of the access may be taken into account together with the other concurrent circumstances to assess the manifestly unfounded or excessive nature of the request."
5. In Article 13, paragraph 4 is replaced by the following:	CZ (Drafting suggestions): In Article 13, ~~paragraph 4 is replaced by~~ the following ***paragraph is added***:

Commission proposal	Drafting suggestions and Comments
	CZ (Comments): CZ **red line:** This new text should not replace current Article 13(4) but complement it. Mere replacement would result in never-ending repetitions of well-known facts that would cause major administrative burden in many contexts.
'4. Paragraphs 1, 2 and 3 shall not apply where ~~the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and~~ there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1 **and the personal data are collected in the context of a direct and clearly circumscribed relationship between data subjects and a controller exercising an activity that is not likely to result in a high risk to the rights and freedoms of data subjects nor involve complex processing operations, the processing of large amounts of personal data, special categories of personal data, or personal data relating to criminal convictions and offences.** **The first subparagraph shall not apply where** ~~, unless~~ the controller **intends to process the data collected from the data subject for other purposes,** transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.'	NL (Drafting suggestions): 4. Paragraphs 1, 2 and 3 shall not apply: **(a) where and insofar as the data subject has the information; or** **(b)** where there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1 and the personal data are collected in the context of a direct and clearly circumscribed relationship between data subjects and a controller exercising an activity that is not likely to result in a high risk to the rights and freedoms of data subjects nor involve complex processing operations, the processing of large amounts of personal data, special categories of personal data, or personal data relating to criminal convictions and offences. The first subparagraph shall not apply where the controller intends to process the data collected from the data subject for other purposes, transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35. NL (Comments): The exemption from Article 13(4) is overwritten by the new proposed exemption. This seems to be a technical error. Unintentionally, this would lead to a significant complication of the rules. Therefore, NL proposes to

Commission proposal	Drafting suggestions and Comments
	split the proposed Article 13(4) in two subparagraphs and to keep the current Article 13(4) in subparagraph 4a. The new exception should be moved to subparagraph 4b. LU (Drafting suggestions): 4. Paragraphs 1 **and** ~~,~~ 2 ~~**and 3**~~ shall not apply where ~~the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and~~ there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1 ***and the personal data are collected in the context of a direct and clearly circumscribed relationship between data subjects and a controller exercising an activity that is not likely to result in a high risk to the rights and freedoms of data subjects nor involve complex processing operations, the processing of large amounts of personal data, special categories of personal data, or personal data relating to criminal convictions and offences, unless*** ~~.~~ ~~***The first subparagraph shall not apply where,***~~ ~~unless~~ the controller ~~***intends to process the data collected from the data subject for other purposes,***~~ transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.' LU (Comments): We note an incoherence between subparagraph 1 and 2 because the first excludes the application of Article 13(3) ("3 should not apply") whereas the second subparagraph includes it again ("intends to process the data collected

Commission proposal	Drafting suggestions and Comments
	from the data subject for other purposes"). We would therefore suggest deleting the reference to paragraph 3 in the first sentence making it thus applicable and tendering "intends to process the data collected from the data subject for other purposes" superfluous. We also preferred the previous wording where the provision had only one paragraph ("unless") and not two subparagraphs. EE (Comments): Estonia supports the amendment. AT (Drafting suggestions): '4. Paragraphs 1, 2 and 3 shall not apply where ~~the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and~~ there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1 ***and the*** *personal data are collected in the context of a direct and clearly circumscribed relationship between data subjects and a controller exercising an activity that is not likely to result in a high risk to the rights and freedoms of data subjects nor involve complex processing operations, ~~the~~* ***large scale*** *processing ~~of large amounts~~ of personal data, special categories of personal data, or personal data relating to criminal convictions and offences.* *The first subparagraph shall not apply where~~, unless~~* the controller *intends to process the data collected from the data subject for other purposes***,** transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.'

Commission proposal	Drafting suggestions and Comments
	AT (Comments): • AT **can support** the compromise proposal on Article 13(4) and Recital 36 GDPR. The proposed amendments provide important clarifications. • We would still prefer the use of the term "**large scale processing of personal data**" as that term is already used in the GDPR, notably in Article 35 – which the proposed Article 13(4) itself refers to – as well as Article 37, and covered by relevant EDPB guidelines. • Alternatively, we would ask the Presidency for the reasoning for using the term "processing of large amounts of personal data" instead of "large scale processing of personal data". FI (Comments): FI can support this proposal. CZ (Comments): CZ would strongly support less restrictive wording of this provision. PL (Drafting suggestions): Drafting proposal: „4. Paragraphs 1, 2 and 3 shall not apply if and to the extent that the data subject already has the information or if the provision of such information proves impossible or, provided the processing is to result in a low risk to data subjects, would involve a disproportionate effort, especially in every-day business. Article 14(5)(b) shall apply accordingly.

Commission proposal	Drafting suggestions and Comments
	Sentence1, 2nd and 3rd alternative shall not apply where the processing concerns personal data referred to in Articles 9 or 10 of this Regulation, or where the personal data are further processed for purposes other than those for which the data were originally collected.". PL (Comments): We maintain our previous position because the current compromise remains excessively complex and may significantly limit the practical application of the proposed exemption, in particular for SMEs. Proposal for amended wording of Article 13(4):
6. In Article 13, paragraph 5 is added:	CZ (Drafting suggestions): In Article 13, ~~paragraph 4 is replaced by~~ the following ***paragraph is added***: CZ (Comments): To cater for inclusion of previous new paragraph, which would become paragraph 5.
'5. When the **further** processing takes place for scientific research purposes **by the same controller and where and insofar as** ~~and~~ the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort ~~subject to the conditions and safeguards referred to in Article 89(1)~~ or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that **further** processing**, subject to the conditions and safeguards referred to**	LU (Comments): We would prefer the initial proposal. AT (Comments): • In principle, AT would be open to this proposal.

Commission proposal	Drafting suggestions and Comments
in Article 89(1), the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.'	• However, in light of the also proposed very broad definition of "scientific research" (see AT comments on Article 4(38) and Article 5(1)b), AT **cannot support it**. • Extended possibilities for processing of personal data for (pseudo-)scientific research purposes would lead to an increase of the volume of personal data processed for this purpose, which would constitute strong interferences with the rights of the data subject. Paired with a limitation of the data subjects' rights this would increase the risk of data protection infringements. FI (Comments): FI can support this proposal. CZ (Comments): CZ would strongly support less restrictive wording of this provision. SE (Drafting suggestions): When the ~~***further***~~ processing takes place for scientific research purposes ***by the same controller and where and insofar as***~~and~~ the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort ~~subject to the conditions and safeguards referred to in Article 89(1)~~ or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of ~~that~~ ~~***further***~~ processing***, subject to the conditions and safeguards referred to in Article 89(1)***, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect

Commission proposal	Drafting suggestions and Comments
	the data subject's rights and freedoms and legitimate interests, including making the information publicly available.' SE (Comments): As previously stressed by Sweden, the exception set out in the proposed paragraph with regards to the possibility to derogate from the obligation of information where such information would render impossible or seriously impair the achievement of the purpose of the scientific research, risks of being too narrow as it only refers to *further processing* whereas the possibility to derogate from the information obligation ***should also*** be applicable ***in the collection phase***.
7. ~~In~~ Article 22~~, paragraphs 1 and 2 are~~ **is** replaced by the following:	AT (Drafting suggestions): ~~7. In Article 22, paragraphs 1 and 2 are **is** replaced by the following:~~ SK (Comments): **SK:** We support this proposal.
'1. ~~A decision which produces legal effects for a~~ **The** data subject ~~or similarly significantly affects him or her may be~~ **shall have the right not to be subject to a decision** based solely on automated processing, including profiling, ~~only where that decision~~ **which produces legal effects concerning him or her or similarly significantly affects him or her, unless such processing**:	LU (Comments): Article 22 of the GDPR has long been regarded as offering limited legal clarity and is frequently perceived as difficult to understand in practice. Moreover, the concrete legal result of an explicit reference to a 'right' not to be subject to an automated decision remain uncertain, a point clearly reflected in the ongoing debate surrounding this provision. We would be more favourable to the initial proposal. EE

Commission proposal	Drafting suggestions and Comments
	(Comments): Estonia supports the amendment. AT (Drafting suggestions): ~~'1. A decision which produces legal effects for a~~ **The** ~~data subject or similarly significantly affects him or her may be~~ **shall have the right not to be subject to a decision** ~~based solely on automated processing, including profiling, only where that decision~~ **which produces legal effects concerning him or her or similarly significantly affects him or her, unless such processing**~~:~~ AT (Comments): • In light of the still pending case in front of the CJEU, C-568/25, we would argue for the deletion of Article 22 from the Digital Omnibus in total. • Furthermore, Article 22 as included in the Proposal is, for all intents and purposes, identical to the current Article 22. The contraction of paragraphs 1 and 2 does not seem sufficient to justify re-adopting Article 22 in its current form. Article 22 should be deleted from the Proposal. FI (Comments): FI can support this proposal. PL (Comments): We maintain our previously submitted comments regarding Article 22(1), as the wording of this provision remains unchanged.

Commission proposal	Drafting suggestions and Comments
	At the same time, we note that the newly added paragraphs 2 and 3 reproduce safeguards already contained in the current Article 22(3) and (4) GDPR. As a result, the proposal maintains the existing status quo. The normative effect of the provision remains essentially identical to that of the current Article 22 GDPR. Given that the Omnibus initiative is intended to simplify and facilitate the application of EU legislation, including for SMEs, it remains unclear what concrete simplification this proposal introduces compared to the current wording of Article 22 GDPR. The proposal largely reproduces the existing structure, safeguards and conditions applicable to automated decision-making, without substantially reducing compliance burdens, addressing the principal interpretative challenges identified in practice, or otherwise providing a significant increase in legal certainty. In this context, the added value of reopening Article 22 within the framework of the Omnibus initiative would benefit from further clarification. Consideration could be given to whether additional clarification of the key concepts and conditions governing automated decision-making would better contribute to the simplification objectives of the initiative while maintaining the current level of protection of data subjects.
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller ~~regardless of whether the decision could be taken otherwise than by solely automated means~~;	EE (Comments): Estonia supports the amendment provided that the qualification “regardless of whether the decision could be taken otherwise than by solely automated means” is addressed in recitals. AT (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;~~ FI (Comments): FI can support this proposal. CZ (Drafting suggestions): (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller **regardless of whether the decision could be taken otherwise than by solely automated means**; CZ (Comments): CZ fully supports the Presidency in return to original structure of Article 22 with the stipulation of a right. However, CZ considers the clarification proposed by the Commission to be still useful and functional. SE (Drafting suggestions): is necessary for entering into, or performance of, a contract between the data subject and a data controller-regardless of whether the decision could be taken otherwise than by solely automated means; SE (Comments): The recital provides for a more generous approach than the text in operative part. The exception described in the Article seems to stipulate that automated decision making must be strictly necessary for the exception to apply. The wording of the recital on the other hand states that fact that the decision can be taken by a human does not preclude the possibility of automated decision

Commission proposal	Drafting suggestions and Comments
	making. Sweden considers that the operative text should be changed to reflect the wording of the recital.
(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or	AT (Drafting suggestions): ~~(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or~~ FI (Comments): FI can support this proposal.
(c) is based on the data subject's explicit consent.	AT (Drafting suggestions): ~~(c) is based on the data subject's explicit consent.~~ FI (Comments): FI can support this proposal.
2. In the cases referred to in points (a) and (c) of paragraph 1, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.	EE (Comments): Estonia supports the amendment. AT (Drafting suggestions): **~~2. In the cases referred to in points (a) and (c) of paragraph 1, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.~~**

Commission proposal	Drafting suggestions and Comments
	FI (Comments): FI can support this proposal.
3. Decisions referred to in paragraph 1 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.'	EE (Comments): Estonia supports the amendment. AT (Drafting suggestions): ~~**3. Decisions referred to in paragraph 1 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.'**~~ FI (Comments): FI can support this proposal.
(7a) In Article 25, paragraphs 1 and 2 are replaced by the following: **'1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, with particular regard to the lists referred to in Article 35(4) and (5), the controller and the processor shall, both at the time of the determination of the means for processing and at the time of the processing itself as applicable, implement, in an effective manner, appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.**	LU (Comments): We would like to get more insight on the reasons for these changes especially regarding the already existing obligations of the data controller and data processor in Article 32 to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. FR (Drafting suggestions): **7b. Article 24 is amended as follows:** **(a) paragraph 1 is replaced by the following:**

Commission proposal	Drafting suggestions and Comments
2. The controller and the processor shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.	'1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, **with particular regard to the lists referred to in Article 35(4) and (5),** the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.' **7c. Article 32 is amended as follows:** **(a) paragraph 1 is replaced by the following:** '1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, **with particular regard to the lists referred to in Article 35(4) and (5),** the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.' FR (Comments):

Commission proposal	Drafting suggestions and Comments
	Les autorités françaises rappellent leur demande aux articles 24 et 32, d'y introduire également une référence aux listes de l'article 35 – en plus des références déjà ajoutées à l'article 25. EE (Drafting suggestions): ~~(7a) In Article 25, paragraphs 1 and 2 are replaced by the following:~~ ~~'1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, with particular regard to the lists referred to in Article 35(4) and (5), the controller and the processor shall, both at the time of the determination of the means for processing and at the time of the processing itself as applicable, implement, in an effective manner, appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.~~ ~~2. The controller and the processor shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.~~ EE (Comments): Estonia does not support adding processor to the subjects of this Article, as this would create an unnecessary imbalance in the relationship in between the

Commission proposal	Drafting suggestions and Comments
	controller and processor. The obligations of the processor are already provided for elsewhere in the articles of GDPR. DK (Comments): DK: regarding the new recital 39a and and the proposed article 25, Denmark understands that it shifts the responsibility for compliance with relevant parts of the GDPR from the controller to the processor. In that case, Denmark can support the provision. However, Denmark cannot support the provision if it merely imposes a burden on the processor that is not offset by a reduction in the burden on the controller. AT (Drafting suggestions): (7a) In Article 25, paragraphs 1 and 2 are replaced by the following: '1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, with particular regard to the lists referred to in Article 35(4) and (5), the controller and the processor shall, both at the time of the determination of the means for processing and at the time of the processing itself as applicable, implement, in an effective manner, appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, **and** to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller and the processor shall implement appropriate technical and organisational measures ~~for ensuring~~ **to ensure** that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected,

Commission proposal	Drafting suggestions and Comments
	the extent of their processing, the period of their storage and their accessibility. In particular, ~~such measures~~ **the controller and the processor** shall ensure that, by default, personal data are not made accessible ~~without the individual's intervention~~ to an indefinite number of natural persons **without the individual's intervention**. AT (Comments): • AT **can support** the amendment but proposes editorial changes. FI (Comments): FI has reservations to add processors in Article 25 without a proper assessment but understand that processors should also bear the responsibility especially in situations where SMEs use processors that provide services with "take it or leave it" conditions. However, this is not a redline. CZ (Drafting suggestions): **(7a) In Article 25, paragraphs 1 and 2 are replaced by the following: '1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, ~~with particular regard to the lists referred to in Article 35(4) and (5),~~ the controller ~~and the processor~~ shall, both at the time of the determination of the means for processing and at the time of the processing itself as applicable, implement, in an effective manner, appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.**

Commission proposal	Drafting suggestions and Comments
	2. The controller ~~and the processor~~ shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. CZ (Comments): CZ is sceptical about this proposal, which is not necessary and does not address any substantial issue. While references to processor might be accepted in light of Article 32 and 83, the reference to lists simply creates interpretative inconsistencies with Articles 24 and 32 GDPR and is contrary to the aims of simplification. CZ could accept even this in the spirit of compromise if accompanied by amendments to Article 49 GDPR reflecting the ES delegation's proposals on tax information exchange. As regards the addition of "and the processor" in both paragraphs, CZ understands the intention of the Presidency. However, current explanation in recital 39a is too vague. CZ could agree to addition of "and the processors" only if recital 39a fully establishes precedence of controller as regards "live processing" as opposed to design of offered products or services (see above). SK (Drafting suggestions): **7a) In Article 25, paragraphs 1 and 2 are replaced by the following: '1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the**

Commission proposal	Drafting suggestions and Comments
	risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, ~~with particular regard to the lists referred to in Article 35(4) and (5),~~ the controller and the processor shall, both at the time of the determination of the means for processing and at the time of the processing itself as applicable, implement, in an effective manner, appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller and the processor shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. SK (Comments): **SK:** We support adding processor in this paragraphs. In our view, it is not neccessary to add reference to the lists referred to in Article 35(4) and (5). SE (Comments): SE has concerns about the addition of *processor* into the provision and whether this addition could affect the division of responsibility between the controller and the processor, since the controller is determining the means of the processing. The corresponding recital states that this is not the intention. Nevertheless, the wording could be interpreted otherwise. PL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): We maintain our previously submitted drafting suggestion: "The allocation of responsibilities between the controller and the processor regarding the implementation of these measures shall be clearly defined, in particular in the contract or other legal act referred to in Article 28(3)." PL (Comments): We maintain our previous concerns regarding the practical allocation of responsibilities between controllers and processors under Article 25. While we acknowledge the intention to reflect current technological and market realities by extending data protection by design and by default obligations to processors, the proposed wording does not sufficiently clarify how responsibilities should be allocated in practice between the parties. Given that the controller remains primarily responsible under the GDPR for ensuring compliance with the Regulation, additional clarification would be beneficial in order to avoid legal uncertainty, overlapping obligations and potential inconsistencies in implementation. This issue becomes particularly relevant where technical and organisational measures are designed, developed or maintained by processors on behalf of multiple controllers. In such situations, greater clarity regarding the respective responsibilities of the parties would contribute to legal certainty and facilitate the practical application of the provision.
8. Article 33 is amended as follows:	SK (Comments): SK: We support this proposal.

Commission proposal	Drafting suggestions and Comments
(a) paragraph 1 is replaced by the following:	
'1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than ~~96~~**72** hours after having become aware of it, notify the personal data breach via the ~~single-entry~~ **national entry** point established pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555 to the supervisory authority competent in accordance with Article 55 and Article 56 **of this Regulation**. Where the notification to the supervisory authority is not made within ~~96~~**72** hours, it shall be accompanied by reasons for the delay.'	LU (Comments): We express our full support for **the initial proposal** extending the deadline for such notifications from 72 to 96 hours. The Commission's rationale behind the extension of the deadline from 72 to 96 hours in the Commission's proposal hours would help data controllers gather more information on the data breaches which would in turn help data protection authorities EE (Drafting suggestions): '1. In the case of a personal data breach that is likely to result in ~~a high~~ **an impactful** risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than ~~96~~72 hours after having become aware of it, notify the personal data breach via the ~~single-entry~~ national entry point established pursuant to Article ~~23a~~23b of Directive (EU) 2022/2555 to the supervisory authority competent in accordance with Article 55 and Article 56 of this Regulation. Where the notification to the supervisory authority is not made within ~~96~~72 hours, it shall be accompanied by reasons for the delay.' EE (Comments): Estonia supports the amendment concerning 72 hours, but the threshold for notification of breaches should be linked to risks, which cannot be considered minor, i.e impactful risks (see also the comment to relevant recital). AT (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	‘1. In the case of a personal data breach that is likely to result in ~~a high risk~~ **an “impactful risk” [“relevant risk”/”increased risk”]** to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than ~~96~~***72*** hours after having become aware of it, notify the personal data breach via the ~~single-entry~~***national entry*** point established pursuant to Article ~~23a~~***23b*** of Directive (EU) 2022/2555 to the supervisory authority competent in accordance with Article 55 and Article 56 ***of this Regulation***. Where the notification to the supervisory authority is not made within ~~96~~***72*** hours, it shall be accompanied by reasons for the delay.’ AT (Comments): • AT **remains sceptical** towards raising the threshold for data breach notifications to the supervisory authority. • A possible compromise could be to use a threshold between “risk” and “high risk”, such as “impactful risk”, “relevant risk”, “increased risk” or similar. • AT generally supports the alignment of time-limits in different legal acts • AT supports maintaining the 72h time limit. FI (Comments): FI can support this proposal. FI supports the high-risk threshold and prefers the current 72 hours. CZ (Drafting suggestions): ‘1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than ~~96~~~~72~~ 96 hours after having become aware of it, notify the personal data breach via the ~~single-entry~~

Commission proposal	Drafting suggestions and Comments
	national entry point established pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555 to the supervisory authority competent in accordance with Article 55 and Article 56 **of this Regulation**. Where the notification to the supervisory authority is not made within ~~9672~~ **96** hours, it shall be accompanied by reasons for the delay.' CZ (Comments): CZ supports, like BE, DE, PL and SE, return to longer time-limit which was not even opposed by EDPB. Longer time period of 96 hours would help in particular the smaller controllers with lesser IT and legal capacities. BE (Comments): We still prefer 96 hours for data breaches in Article 3(8) of the Omnibus, article 33 of GDPR SE (Drafting suggestions): In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than **9672** ~~hours~~ after having become aware of it, notify the personal data breach via the ~~single entry~~ **national entry** point established pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555 to the supervisory authority competent in accordance with Article 55 and Article 56 **of this Regulation**. Where the notification to the supervisory authority is not made within **9672** ~~hours~~, it shall be accompanied by reasons for the delay.'

Commission proposal	Drafting suggestions and Comments
	SE (Comments): Sweden is in favour of the Commission's proposal to extend this deadline to 96 hours as we believe that this would contribute to the overall objective of alleviating administrative burdens to businesses. Further, the relevant wording seems to assume the establishment of a national entry point. In this regard, SE would like to refer to the comments made below in relation to the relevant articles in Directive (EU) 2022/2555. PL (Drafting suggestions): We maintain our previous drafting suggestion to replace the deadline of 72 hours with 96 hours in Article 33(1). PL (Comments): Extending the notification deadline could also improve the quality and proportionality of breach notifications. In practice, controllers faced with a relatively short notification deadline may be incentivised to notify incidents at a very early stage of the investigation in order to avoid the risk of non-compliance, even where it remains unclear whether the incident meets the threshold for notification. Providing additional time would allow controllers to conduct a more thorough assessment of the incident and its potential impact on the rights and freedoms of natural persons before deciding whether notification is required. This could contribute to reducing precautionary or defensive notifications and enable supervisory authorities to focus their resources on breaches that genuinely meet the notification threshold.

Commission proposal	Drafting suggestions and Comments
	Furthermore, the practical challenges associated with assessing incidents within 72 hours may be particularly significant where breaches occur immediately before weekends, public holidays or other periods during which the availability of relevant personnel may be limited. ES (Comments): **Spain.** we agree with 72 h.
(b) the following paragraph is added:	
'1a. Until the establishment of the ~~single-entry~~ **national entry** point pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555, controllers shall continue to notify personal data breaches directly to the competent supervisory authority in accordance with Article 55 and Article 56 **of this Regulation**.'	EE (Comments): Estonia supports the amendment
(c) the following paragraphs are added:	
'6. The Board shall ~~prepare and transmit to the Commission a proposal for~~ **establish and make public** a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as ~~for~~ a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person **and a list of the circumstances in which it is not likely to result in such a high risk. The template and lists**~~. The proposals~~ shall be ~~submitted to the Commission~~ **available** within [OP date = nine months of the entry into application of this Regulation]. The Commission ~~after due consideration reviews it, as necessary, and is empowered to~~ **may** adopt ~~it~~ **the template as established by the Board** by way of an implementing act**,** in accordance with the examination procedure set out in Article 93(2).	NL (Drafting suggestions): 6. The Board shall establish and make public a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as ~~for~~ a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person and a list of the circumstances in which it is not likely to result in such a high risk. The template and lists shall be available within [OP date = nine months of the entry into application of this Regulation]. ~~The Commission may adopt the template as established by the Board by way of an implementing act, in accordance with the examination procedure set out in Article 93(2).~~

Commission proposal	Drafting suggestions and Comments
	NL (Comments): NL notes that the proposed Article 33(6) suggests that the Commission may only put in an implementing act what the EDPB has established as a template. However, the Commission cannot be required to not make any changes in the template, as the Commission has the final say on the text of the implementing act. NL proposes to give the final say, *regarding both the template and the lists on the notification of data breaches*, to the (independent) EDPB, as this would provide needed legal certainty, while avoiding the risk of more political decision-making. EE (Drafting suggestions): '6. The Board shall ~~prepare and transmit to the Commission a proposal for~~ establish and make public a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as ~~for~~ a list of the circumstances in which a personal data breach is likely to result in **~~a high~~ an impactful** risk to the rights and freedoms of a natural person and a list of the circumstances in which it is not likely to result in such a **~~high~~** risk. The template and lists~~. The proposals~~ shall be ~~submitted to the Commission~~ available within [OP date = nine months of the entry into application of this Regulation]. **~~The Commission may adopt the template as established by the Board by way of an implementing act, in accordance with the examination procedure set out in Article 93(2).~~** EE (Comments): Regarding the "common template" - see also the proposed NIS2 Article 23c (3) (a) and comments related to said paragraph + comment on NIS2 Article 23 amendments (at the introduction).

Commission proposal	Drafting suggestions and Comments
	Estonia does not support the amendment as regards the division of competences in between EDPB and the Commission. In a situation where the Board's guidelines can be updated quickly in response to newly emerging possibilities, there is a risk that the guidelines may recommend an updated approach, while the Commission's implementing regulation in force contains outdated information. Amending both the EDPB guidelines and the implementing regulation will be a lengthy process and can result in different outcomes. This could result in a situation where controllers are unable to use up-to-date measures without committing a breach, thereby jeopardising the protection of individuals' personal data. We do understand that the EDPB's guidelines may be challenged in ECJ, but providing that its guidelines must be validated by an implementing regulation will jeopardise the EDPB's autonomy. We also propose amendments as to align the provision with our proposal for Article 33 (1). AT (Drafting suggestions): '6. The Board shall ~~prepare and transmit to the Commission a proposal for~~*~~establish and make public~~* **publish** **a)** a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1, **b)** ~~as well as for~~ a list of the circumstances in which a personal data breach is likely to result in **a high risk** to the rights and freedoms of a natural person and a list of the circumstances in which it is not likely to result in such a ~~**high**~~ risk **and** **c) a list of the circumstances in which a personal data breach is likely to result in an "impactful risk" ["relevant risk"/"increased risk"] to the rights and freedoms of a natural person and a list of the circumstances in which it is not likely to result in such risk**. The template and lists~~. The proposals~~ shall be ~~submitted to the Commission~~available within [OP date = nine months of the entry into

Commission proposal	Drafting suggestions and Comments
	application of this Regulation]. ~~**The Commission after due consideration reviews it, as necessary, and is empowered to*may* adopt it*the template as established by the Board* by way of an implementing act, in accordance with the examination procedure set out in Article 93(2).**~~ AT (Comments): • AT **continues to support** the issuing of a common template for data breach notifications and the lists of circumstances relating to the risk threshold by the EDPB. • **The task should remain with the EDPB. The wording should be adapted accordingly ("*publish*").** • The proposed wording regarding the risk threshold is designed to align with the AT proposal for Article 33(1). • A list of circumstances requiring notification under Article 33 as well as under Article 34 should be provided. • For structural reasons, provisions regarding tasks of the EDPB should be moved to Article 70 GDPR, where all tasks of the EDPB are currently regulated. FI (Comments): FI supports that the EDPB establishes and makes public a common template and lists. Concerning possible implementing acts, FI has a question what happens when the EDPB revises and changes the template and lists, but the legally binding implementing acts have yet not been changed. Could this undermine the role of the EDPB and weaken the compliance of EDPB guidance. FI welcomes that the Council Legal Services would clarify this. If there are no objections from the Council Legal Services, FI can support implementing acts. However, if there are objections or reservations, FI proposes to leave

Commission proposal	Drafting suggestions and Comments
	this matter for EDPB templates and lists and to delete the possibility for implementing acts. CZ (Drafting suggestions): '6. The Board shall ~~prepare and transmit to the Commission a proposal for~~ **establish and make public** a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as ~~for~~ a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person **and a list of the circumstances in which it is not likely to result in such a high risk. The template and lists**~~. The proposals~~ shall be ~~submitted to the Commission~~ **available** within [OP date = nine months of the entry into application of this Regulation]. The Commission ~~after due consideration reviews it, as necessary, and is empowered to~~ **may** adopt ~~it~~ **the template duly reviewed, as necessary** ~~as established by the Board~~ by way of an implementing act**,** in accordance with the examination procedure set out in Article 93(2). CZ (Comments): CZ may, in the spirit of compromise, accept more pronounced role of EDPB. SE (Drafting suggestions): The Board shall prepare and transmit to the Commission a proposal for ~~***establish and make public***~~ a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as ~~for~~ a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person ***and a list of the circumstances in which it is not likely to result in such a high risk. The template and lists***~~. The proposals~~ shall be submitted to the

Commission proposal	Drafting suggestions and Comments
	Commission***available*** within [OP date = nine months of the entry into application of this Regulation]. The Commission after due consideration reviews it, as necessary, and is empowered to***may*** adopt ~~it~~***~~the template as established by the Board~~*** by way of an implementing act**,** in accordance with the examination procedure set out in Article 93(2). SE (Comments): Sweden supports the proposal to allow for the Commission to adopt implementing acts in this regard in accordance with the comitology procedure set out in Article 93(2). As previously stated, in order to ensure effectiveness in the procedure, the Commission should be given a margin of discretion and be able to review the proposals as necessary made by the board. PL (Drafting suggestions): '6. The Board shall ~~prepare and transmit to the Commission a proposal for~~ **establish and make public** a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as ~~for~~ a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person **and a list of the circumstances in which it is not likely to result in such a high risk. The template and lists**~~. The proposals~~ shall be ~~submitted to the Commission~~ **available** within [OP date = nine months of the entry into application of this Regulation]. The Commission ~~after due consideration reviews it, as necessary, and is empowered to~~ **may** adopt ~~it~~ **the template** ~~**as established by the Board**~~ by way of an implementing act**,** in accordance with the examination procedure set out in Article 93(2). PL

Commission proposal	Drafting suggestions and Comments
	(Comments): The procedure of adoption of the implementing act should not be limited, as Member States should be able to present their positions.
7. The template and ~~the list~~ **lists** referred to in paragraph 6 shall be reviewed at least every three years and updated where necessary. The ~~Board shall submit its assessment and possible proposals for updates to the~~ Commission ~~in due time. The Commission after due consideration of the proposals reviews them and is empowered to~~ **may** adopt any updates **of the template by way of an implementing act** following the procedure **referred to** in paragraph 6.'	NL (Drafting suggestions): 7. The template and lists referred to in paragraph 6 shall be reviewed at least every three years and updated where necessary. ~~The Commission may adopt any updates of the template by way of an implementing act following the procedure referred to in paragraph 6.'~~ NL (Comments): See Article 33(6). EE (Drafting suggestions): 7. The template and **lists** referred to in paragraph 6 shall be reviewed at least every three years and updated where necessary. ~~**The Commission may adopt any updates of the template by way of an implementing act following the procedure referred to in paragraph 6.'**~~ EE (Comments): See previous comment. AT (Drafting suggestions): 7. The template and ~~the list~~***lists*** referred to in paragraph 6 shall be reviewed at least every three years and updated where necessary. ~~**The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the**~~

Commission proposal	Drafting suggestions and Comments
	~~proposals reviews them and is empowered to~~*~~may~~* ~~adopt any updates~~ *~~of the template by way of an implementing act~~* ~~following the procedure~~ *~~referred to~~* ~~in paragraph 6.~~~~'~~ AT (Comments): • AT **does not support** the proposed new competence of the EC to adopt implementing decisions regarding data breaches. In our opinion, it is unfit for purpose and appears to run counter to the established system for guidelines, recommendations and best practices (see also comment regarding Article 35(6a) below). FI (Comments): FI supports that the EDPB establishes and makes public a common template and lists. Concerning possible implementing acts, FI has a question what happens when the EDPB revises and changes the template and lists, but the legally binding implementing acts have yet not been changed. Could this undermine the role of the EDPB and weaken the compliance of EDPB guidance. FI welcomes that the Council Legal Services would clarify this. If there are no objections from the Council Legal Services, FI can support implementing acts. However, if there are objections or reservations, FI proposes to leave this matter for EDPB templates and lists and to delete the possibility for implementing acts.
9. Article 35 is amended as follows:	SK (Comments): **SK:** We support this proposal. PL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): We maintain our previously submitted drafting suggestions. PL (Comments): We maintain our previous concerns regarding the governance framework proposed in Article 35. While the objective of increasing harmonisation and reducing fragmentation in the application of data protection impact assessment requirements across the Union is supported, questions remain regarding the legal status and practical effects of the lists, template and methodology established and published by the Board. Given the central role that these instruments would play in the application of the DPIA framework across the Union, it is important to ensure that they provide a sufficient degree of legal certainty and effectively support a consistent application of the Regulation. We also note that the proposed reference to the lists referred to in Article 35(4) and (5) in Article 25 further increases the practical significance of those lists. This reinforces the importance of ensuring a clear and coherent framework governing their establishment, review and application.
(a) paragraphs 4, 5 and 6 are replaced by the following:	
‘4. The Board shall ~~prepare and transmit to the Commission a proposal for~~ **establish and make public** a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.	EE (Comments): Estonia supports the amendment. AT (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	'4. The Board shall ~~prepare and transmit to the Commission a proposal for~~ **publish** a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. AT (Comments): • AT **continues to support** harmonisation with regard to the data protection impact assessment and welcomes that the respective competences are assigned to the EDPB. • For structural reasons, all respective provisions should be moved to Article 70 GDPR, where all tasks of the EDPB are regulated FI (Comments): FI can support this proposal and supports that the EDPB establishes lists. SE (Drafting suggestions): The Board shall prepare and transmit to the Commission a proposal for ***~~establish and make public~~*** a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. SE (Comments): Sweden supports the proposal to allow for the Commission to adopt implementing acts with lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and which processing operations for which no data protection impact assessment is required in accordance with the comitology procedure set out in Article 93(2).

Commission proposal	Drafting suggestions and Comments
5. The Board shall ~~prepare and transmit to the Commission a proposal for~~ **establish and make public** a list of the kind of processing operations for which no data protection impact assessment is required.	EE (Comments): Estonia supports the amendment. AT (Drafting suggestions): 5. The Board shall ~~prepare and transmit to the Commission a proposal for~~*establish and make public* **publish** a list of the kind of processing operations for which no data protection impact assessment is required. AT (Comments): • Move to Article 70 (see comment on Article 35(4) above) • The tasks referred to in Paragraphs 4, 5 and 6 should remain with the EDPB (see comment on Article 33(7) above). The wording should be adapted accordingly. FI (Comments): FI can support this proposal and supports that the EDPB establishes lists. SE (Drafting suggestions): The Board shall prepare and transmit to the Commission a proposal for ~~***establish and make public***~~ a list of the kind of processing operations for which no data protection impact assessment is required.
6. The Board shall ~~prepare and transmit to the Commission a proposal for~~ **establish and make public** a common template and a common methodology for conducting data protection impact assessments.'	EE (Comments): Estonia supports the amendment. AT

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): 6. The Board shall ~~prepare and transmit to the Commission a proposal for~~*~~establish and make public~~* **publish** a common template and a common methodology for conducting data protection impact assessments.' AT (Comments): • Move to Article 70 (see comment on Article 35(4) above). • The tasks referred to in Paragraphs 4, 5 and 6 should remain with the EDPB (see comment on Article 33(7) above). The wording should be adapted accordingly. FI (Comments): FI can support this proposal and supports that the EDPB establishes lists. SE (Drafting suggestions): The Board shall prepare and transmit to the Commission a proposal for ***~~establish and make public~~*** a common template and a common methodology for conducting data protection impact assessments.'
(b) the following ~~paragraphs are~~ **paragraph is** inserted:	
'6a. ~~The proposals for~~ The lists referred to in paragraphs 4 and 5 and ~~for~~ the template and methodology referred to in paragraph 6 shall be ~~submitted to the Commission~~ **published** within [OP date = 9 months of the entry into application of this Regulation]. The Commission ~~after due consideration reviews them, as necessary, and is empowered to~~ **may** adopt ~~them~~ **the template as established by the Board** by way of an implementing act**,** in accordance with the examination procedure set out in Article 93(2).	NL (Drafting suggestions): 6a. The lists referred to in paragraphs 4 and 5 and the template and methodology referred to in paragraph 6 shall be published within [OP date = 9 months of the entry into application of this Regulation]. ~~The Commission may adopt the template as established by the Board by way of an implementing act, in accordance with the examination procedure set out in Article 93(2).~~

Commission proposal	Drafting suggestions and Comments
	NL (Comments): NL notes that the proposed Article 35(6a) and 35(6b) suggest that the Commission may only put in an implementing act what the EDPB has established as a template. However, the Commission cannot be required to not make any changes in the template, as the Commission has the final say on the text of the implementing act. NL proposes to give the final say, regarding *both the template and the DPIA lists*, to the (independent) EDPB, as this would provide needed legal certainty, while avoiding the risk of more political decision-making. EE (Drafting suggestions): '6a. ~~The proposals for~~ The lists referred to in paragraphs 4 and 5 and ~~for~~ the template and methodology referred to in paragraph 6 shall be ~~submitted to the Commission~~ published within [OP date = 9 months of the entry into application of this Regulation]. ~~**The Commission may adopt the template as established by the Board by way of an implementing act, in accordance with the examination procedure set out in Article 93(2).**~~ EE (Comments): See the justifications in the comments above (Article 33 (6) of the GDPR). AT (Drafting suggestions): '6a. The ~~**proposals for the**~~ lists referred to in paragraphs 4 and 5 and for the template and methodology referred to in paragraph 6 shall be ~~submitted to the Commission~~*published* within [OP date = 9 months of the entry into application of this Regulation]. ~~**The Commission after due consideration reviews them, as necessary, and is empowered to*may* adopt them*the***~~

Commission proposal	Drafting suggestions and Comments
	~~***template as established by the Board* by way of an implementing act, in accordance with the examination procedure set out in Article 93(2).~~ AT (Comments): • Move to Article 70 (see comment on Article 35(4) above). • The tasks referred to in Paragraphs 4, 5 and 6 should remain with the EDPB (see comment on Article 33(7) above). The wording should be adapted accordingly. FI (Comments): FI supports that the EDPB establishes and makes public a common template and lists. Concerning possible implementing acts, FI has a question what happens when the EDPB revises and changes the template and lists, but the legally binding implementing acts have yet not been changed. Could this undermine the role of the EDPB and weaken the compliance of EDPB guidance. FI welcomes that the Council Legal Services would clarify this. If there are no objections from the Council Legal Services, FI can support implementing acts. However, if there are objections or reservations, FI proposes to leave this matter for EDPB templates and lists and to delete the possibility for implementing acts. CZ (Drafting suggestions): '6a. ~~The proposals for~~ The lists referred to in paragraphs 4 and 5 and ~~for~~ the template and methodology referred to in paragraph 6 shall be ~~submitted to the Commission~~ **published** within [OP date = 9 months of the entry into application of this Regulation]. The Commission ~~after due consideration~~

Commission proposal	Drafting suggestions and Comments
	~~reviews them, as necessary, and is empowered to~~ **may** adopt ~~them~~ **the template** **duly reviewed, as necessary** ~~**as established by the Board**~~ by way of an implementing act, in accordance with the examination procedure set out in Article 93(2). CZ (Comments): CZ may, in the spirit of compromise, accept more pronounced role of EDPB. SE (Drafting suggestions): The proposals for the lists referred to in paragraphs 4 and 5 and for the template and methodology referred to in paragraph 6 shall be submitted to the Commission~~***published***~~ within [OP date = 9 months of the entry into application of this Regulation]. The Commission ***after due consideration*** reviews them, as necessary, and is empowered to***may*** adopt ~~them~~***the template*** ~~***as established by the Board***~~ by way of an implementing act**,** in accordance with the examination procedure set out in Article 93(2). SE (Comments): Sweden supports allowing for the Commission to adopt the template as an implementing act in accordance with the comitology procedure set out in Article 93(2). In order to ensure effectiveness in the procedure, the Commission should be given a margin of discretion and be able to review the proposals made by the board. PL (Drafting suggestions): The Commission ~~after due consideration reviews them, as necessary, and is empowered to~~ **may** adopt ~~them~~ **the template** ~~**as established by the Board**~~

Commission proposal	Drafting suggestions and Comments
	by way of an implementing act**,** in accordance with the examination procedure set out in Article 93(2). PL (Comments): The procedure of adoption of the implementing act should not be limited, as Member States should be able to present their positions.
6b. The lists and the template and methodology referred to in paragraph 6a- shall be reviewed **by the Board** at least every three years and updated where necessary. The ~~Board shall submit its assessment and possible proposals for updates to the~~ Commission ~~in due time. The Commission after due consideration of the proposals reviews them and is empowered to~~ **may** adopt any updates **of the template by way of an implementing act** following the procedure **referred to** in paragraph 6a.	NL (Drafting suggestions): 6b. The lists and the template and methodology referred to in paragraph 6a- shall be reviewed by the Board at least every three years and updated where necessary~~. The Commission may adopt any updates of the template by way of an implementing act following the procedure referred to in paragraph 6a.~~ NL (Comments): See Article 35(6a). EE (Drafting suggestions): 6b. The lists and the template and methodology referred to in paragraph 6a- shall be reviewed by the Board at least every three years and updated where necessary. ~~**The Commission may adopt any updates of the template by way of an implementing act following the procedure referred to in paragraph 6a.**~~ EE (Comments): See the justifications in the comments above (Article 33 (6) of the GDPR). AT

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): 6b. The lists and the template and methodology referred to in paragraph 6a- shall be reviewed ***by*** *the Board* at least every three years and updated where necessary. ~~**The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to*** ~~***may***~~ ~~**adopt any updates** ***of the template by way of an implementing act*** **following the procedure** ***referred to*** **in paragraph 6a.**~~ AT (Comments): • Move to Article 70 (see comment on Article 35(4) above). FI (Comments): See comment above.
6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required established and made public by supervisory authorities remain valid until the ~~Commission adopts the implementing act~~ **Board establishes and makes public the lists** referred to in paragraph ~~6a~~**4 and 5**.'	EE (Comments): Estonia supports the amendment. AT (Drafting suggestions): 6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required established and made public by supervisory authorities remain valid until the ~~Commission adopts the implementing act~~*Board* ~~***establishes and makes public***~~ ***publishes*** *the lists* referred to in paragraph ~~6a~~***4 and 5***. AT (Comments):

Commission proposal	Drafting suggestions and Comments
	• Move to Article 70 (see comment on Article 35(4) above). • The tasks referred to in Paragraphs 4, 5 and 6 should remain with the EDPB (see comment on Article 33(7) above). The wording should be adapted accordingly. FI (Comments): FI can support this proposal
(9a) In Article 37, paragraph 7 is replaced by the following: **'7. The controller or the processor shall publish the contact details of the data protection officer.'**	NL (Drafting suggestions): ~~**(9a) In Article 37, paragraph 7 is replaced by the following:**~~ ~~**'7. The controller or the processor shall publish the contact details of the data protection officer.'**~~ NL (Comments): NL is concerned about this proposed deletion of the current obligation to notify the contact details of a Data Protection Officer to the Supervisory Authority. This change could undermine the independent position of the Data Protection Officer (DPO) as well as the performance of the tasks of the external supervisory authority. In the event of a data breach, both must be able to liaise (quickly) with each other. In case of an investigation, the supervisory authority should be able to contact the (correct) DPO without alerting the organization for which the DPO works. Neither the DPO nor the supervisory should be dependent, in terms of their position or the performance of their duties, on any whims of the organization concerned, caused by whether or not the latter reports the DPO's contact details to the supervisory authority or by (seriously) delaying this process. LU

Commission proposal	Drafting suggestions and Comments
	(Comments): Given the tangible benefits provided by notifying Data Protection Authorities of DPO contact details, it is difficult to see what added value would result from removing this obligation - either for the authorities themselves or for data controllers. Removing it would probably weaken transparency and the effectiveness of DPO–DPA communication channels. EE (Drafting suggestions): (9a) In Article 37, paragraph 7 is replaced by the following: '7. The controller or the processor shall publish the contact details of the data protection officer **and communicate them to the supervisory authority**.' EE (Comments): Estonia does not support the amendment, as it would significantly increase the workload of the supervisory authority, which would then have to verify all public authorities and businesses subject to the obligation to appoint a data protection officer, rather than contacting only those that have failed to appoint one. Also, this can weaken the position of DPOs. AT (Comments): • AT **is open** to an amendment to Article 37(7) but emphasises that any changes must still ensure that data protection authorities are still able to easily find and contact the competent data protection officer without delay or additional administrative burden. MT (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~***(9a) In Article 37, paragraph 7 is replaced by the following:***~~ ~~***'7.The controller or the processor shall publish the contact details of the data protection officer.'***~~ MT (Comments): We do not agree with the deletion of the requirement to communicate the DPO contact details to the supervisory authority in Article 37(7) GDPR. Removing the requirement to communicate the DPO's contact details to the supervisory authority would not meaningfully reduce the administrative burden on controllers and therefore does not genuinely simplify compliance obligations. Where a controller is required to designate a DPO, it will already have identified that person or function and will necessarily hold the relevant contact details. Transmitting those details to the authority is a minimal one-off or occasional administrative step. By contrast, maintaining the requirement serves an important practical purpose: it enables supervisory authorities to contact the DPO directly and efficiently, without first having to approach other parts of the organisation or rely on publicly available information, which may be absent, outdated, or directed to general inboxes. Removing the obligation would therefore create inefficiencies for supervisory authorities while offering only negligible relief to controllers. FI (Comments): FI is not sure of this proposal to remove the requirement to communicate contact details to DPAs. However, this is not a redline either. SK (Comments):

Commission proposal	Drafting suggestions and Comments
	SK: We propose that this provision remain unchanged. We believe that it is beneficial for DPA to have of contact details of DPO and also have overview of whether controller/processor has designated DPO, when was DPO designation or dismissed, etc. SE (Comments): No comments. PL (Drafting suggestions): We suggest maintaining a mechanism enabling supervisory authorities to receive the contact details of the data protection officer, including in a simplified form. PL (Comments): We do not support the complete removal of the obligation to communicate the contact details of the data protection officer to the supervisory authority. Under the GDPR framework, the data protection officer is not merely a public contact point of the organisation but plays a specific role in facilitating cooperation between controllers or processors and supervisory authorities. In particular, Article 39(1)(d) and (e) GDPR expressly provide that the data protection officer shall cooperate with the supervisory authority and act as a contact point for the supervisory authority on issues relating to processing. Against this background, the complete removal of any mechanism enabling supervisory authorities to receive the contact details of newly designated data protection officers appears difficult to reconcile with the role assigned to the DPO elsewhere in the GDPR.

Commission proposal	Drafting suggestions and Comments
	The proposed amendment may weaken effective and continuous cooperation between supervisory authorities and data protection officers, which constitutes an important element of the supervisory framework established by the GDPR. The DPO does not merely serve as a contact point for specific proceedings or incidents but also acts as a natural counterpart for supervisory authorities in the ongoing application of data protection rules. Supervisory authorities perform a number of tasks that require regular communication with DPOs, including providing guidance, sharing information on regulatory and interpretative developments, organising training and awareness-raising activities, and supporting compliance with data protection requirements. The effective performance of these tasks requires supervisory authorities to have access to up-to-date information regarding designated DPOs. The complete removal of the obligation to communicate DPO contact details to supervisory authorities may result in situations where supervisory authorities are not informed about newly designated DPOs or changes concerning existing DPOs. As a consequence, the regular and continuous cooperation between supervisory authorities and DPOs envisaged by the GDPR may be significantly hindered. This is particularly relevant in relation to newly established organisations required to designate a DPO and situations involving changes in the person performing that function. The availability of up-to-date DPO contact details may also be particularly relevant in situations requiring prompt interaction, including personal data breaches, ongoing supervisory procedures or other circumstances where timely communication between the supervisory authority and the organisation is important.

Commission proposal	Drafting suggestions and Comments
	For these reasons, maintaining at least a simplified mechanism for communicating DPO contact details to supervisory authorities should be considered. ES (Comments): **Spain.** Notifying the Data Protection Authority (DPA) is a very simple process, as it is solely a communication. Therefore, we strongly disagree with eliminating the DPO's notification to the DPA. The information the DPA has about DPOs is crucial for maintaining a relationship with them: organizing informational and training events, communications, etc.
10. The following article is added:	FR (Drafting suggestions): **10a. Article 40, paragraph 2 is amended as follows:** 2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: (a) fair and transparent processing; (b) the legitimate interests pursued by controllers in specific contexts; (c) the collection of personal data; (d) the pseudonymisation of personal data; (e) the information provided to the public and to data subjects; (f) the exercise of the rights of data subjects;

Commission proposal	Drafting suggestions and Comments
	(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained; (h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32; (i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; (j) the transfer of personal data to third countries or international organisations; or (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79. **The Commission may also prepare codes of conduct, or amend or extend such codes in relation to point d) of this parahraph.** **Article 40, paragraph 5 is amended as follows:** 7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55, ~~**shall**~~ before approving the draft code, amendment or extension, **or the European Commission with regards to a draft code prepared pursuant to paragraph 2 point d) shall** submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

Commission proposal	Drafting suggestions and Comments
	FR (Comments): **Les autorités françaises rappellent qu'elles proposent l'introduction d'une nouvelle possibilité pour la Commission de proposer des codes de conduite en matière de pseudonymisation en s'appuyant sur la procédure déjà existante dans le RGPD pour permettre, sur ce sujet où les attentes sont très fortes et transversales, de ne pas faire peser la charge du développement de cet outil sur un responsable de traitement seul, mais d'en partager l'élaboration en permettant à la Commission de proposer un outil nourri de la contribution des opérateurs. Les amendements correspondants à l'article 40 seraient très limités et ciblés.**
'Article ~~41a~~**29a - Application of pseudonymisation and identification of a natural person**	NL (Drafting suggestions): Article 29a - Application of pseudonymisation**, anonymisation** and identification of a natural person NL (Comments): Since the opinion of the EDPB in the new compromise text also would pertain to anonymisation, this could also be expressed in the heading of Article 29a. MT (Comments): See the comment on recital 27a.

Commission proposal	Drafting suggestions and Comments
	Should this Article be maintained, we question whether it would be more appropriate to include this article right after article 32 under Section II (Security of processing) of Chapter IV GDPR (instead of Section 1) since as stated in that article, pseudonymisation is a measure to ensure a level of security appropriate to the risk. FI (Comments): FI can support the proposed Article 29a as well as recitals 27a and 27b. FI primarily supports that there are no changes to the definition for personal data. Taking account of the discussion in the Antici Group on 27th May, FI understands that there is a need to discuss this matter further, possibly in Coreper. Concerning the proposed Article 29a as well as recitals 27a and 27b, FI welcomes that the Presidency has unified the wording with the GDPR. It is important that the EDPB issues an opinion on pseudonymisation. FI can support the compromise proposal. FI supports that there are no implementing acts on pseudonymisation. Alternatively, FI can accept implementing acts but only acts that are technical in nature and/or would only "codify" the EDPB guidance on the matter (similarly as with data breach notification templates and high-risk lists). BE (Comments): BE asks for the reintroduction of the sentence : *Personal data which have undergone pseudonymisation, which could be attributed to a natural person*

Commission proposal	Drafting suggestions and Comments
	by the use of additional information, should be considered to be information on an identifiable natural person SK (Comments): **SK:** We understand that there is a need to reflect the conclusions of the CJEU, but we do not support this new article 29a. In our view, paragraph 1 and 1a are already in GDPR in similar wording - in article 32 paragraph 1 and in recital 26. We disagree with the new task of the Board to issue and opinion under article 64 (2) on this matter. We believe that for this matter it is better for the Board to issue guidelines, recommendations or best practises. It would be better for the Board to work on this issue without legal deadlines. In case of an opinion, there is no time for public consultation. In case of guidelines, Board can organise a public consultation or organise a stakeholder event. We propose to delete this article, article 70(1)(hcb) and recital 27a. PL (Comments): We see a need for further discussions on a technical level. Clarification is necessary regarding the relationship between pseudonymisation, anonymisation and the assessment of whether a natural person is identifiable for the purposes of the GDPR. In particular, paragraph 2 refers to situations in which the application of pseudonymisation may prevent persons other than the controller from identifying a data subject, in such a way that, for them, the data subject is not or is no longer identifiable. While this approach reflects issues already discussed in the case law of the Court of Justice of the European Union and in data protection practice, it continues to raise important interpretative questions regarding the scope of application of the GDPR and the assessment of identifiability from the perspective of different actors.

Commission proposal	Drafting suggestions and Comments
	It is therefore important to ensure that the provision is interpreted consistently with Recital 26 GDPR and existing CJEU case law, in particular as regards the assessment of whether means reasonably likely to be used for identification are available to the entity processing the data. Further clarification is also needed regarding the practical consequences of situations where pseudonymised data may not enable the identification of a natural person from the perspective of a particular recipient, while remaining potentially identifiable for other entities, including entities in third countries, possessing additional information, resources or technical capabilities. In such circumstances, it is important to ensure that the interpretation of Article 29a does not inadvertently reduce the level of protection applied to pseudonymised data or create incentives to treat such data as posing no meaningful privacy risks. Consideration should be given to the fact that pseudonymised datasets may still be exposed to unauthorised disclosure, further transfers or combination with other datasets, potentially enabling the identification of natural persons by third parties. Further clarification of these aspects would contribute to legal certainty and a more consistent application of the GDPR.
(1) ~~The Commission may adopt implementing acts to specify means and criteria to determine whether data resulting from~~ **Controllers and processors may apply** pseudonymisation ~~no longer constitutes~~ **to** personal data ~~for certain entities~~ **in order to reduce the risks to the data subjects concerned and to help meet their obligations under this Regulation**.	EE (Comments): Estonia supports the amendment. CZ (Comments): CZ can accept this paragraph in the spirit of compromise. SE (Comments):

Commission proposal	Drafting suggestions and Comments
	Sweden is in favour of to the ambition to provide greater legal certainty to the notion of pseudonymisation. If the rationale of the said provision is to stipulate that pseudonymisation is to be considered an appropriate safeguard than it should be considered to also include anonymisation. With reference to our comments in relation to Article 4(1), Sweden considers it to be beneficial to codify relevant jurisprudence in Article 4(1) of the GDPR as other legal acts refer to this definition. However, we remain flexible to put the drafted suggestion in a separate article, such as Article 29a.
1a. To determine whether a natural person is identifiable, account shall be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.	EE (Comments): Estonia supports the amendment. CZ (Comments): CZ can accept this paragraph in the spirit of compromise. SE (Comments): The reference to “another person” in the last sentence reflects the proposed wording of recital 26 of the GDPR. However, this addition into the operative text should not result in a stricter application than foreseen by the SRB-judgment, cf. paras. 86-87 of the SRB-judgment where court states i.a. that the recital in question only refers to persons who have or may have access to the means reasonably likely to be used for the purposes of identifying the data subject ES

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): (ES Drafting suggestions): ***Article 49 Derogations for specific situations*** *1. (...)* *Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.* ***The requirement that the transfer be non-repetitive shall not apply to transfers based on point (d) of the first subparagraph, where such transfers are necessary for important reasons of public interest recognised in Union law or in the law of a Member State, including transfers carried out pursuant to international or administrative agreements on mutual assistance or cooperation.*** ES (Comments): (ES Comments): The purpose of this amendment is to clarify and specify the scope of the derogation for important reasons of public interest laid down in Article 49 of

Commission proposal	Drafting suggestions and Comments
	Regulation (EU) 2016/679, in particular as regards international data transfers carried out in the context of periodic exchanges of information between public authorities. The proposed amendment clarifies that transfers necessary for important reasons of public interest under Article 49(1)(d), including those carried out pursuant to international or administrative cooperation agreements, may in practice take place on a recurring basis. It therefore specifies that the requirement of non-repetitiveness, which applies to the residual ground of compelling legitimate interests, should not be understood as limiting such public interest transfers. This clarification does not affect the exceptional nature of Article 49 derogations, which remain subject to strict necessity, proportionality and appropriate safeguards ensuring a high level of protection of personal data.
(2) ~~For the purpose of paragraph 1 the Commission~~ **The Board** shall~~:~~ **issue an opinion, in accordance with Article 64(2) of this Regulation, addressing the application of pseudonymisation and anonymisation, including related technical and organisational measures, and specifying means and criteria to determine whether and when the application of pseudonymisation to personal data may effectively prevent persons other than the controller from identifying a data subject, in such a way that, for them, the data subject is not or is no longer identifiable.**	NL (Drafting suggestions): (2) The Board shall issue an opinion, in accordance with Article 64(2) of this Regulation, addressing the application of pseudonymisation and anonymisation, including related technical and organisational measures, and specifying means and criteria to determine whether and when the application of pseudonymisation to personal data may effectively prevent persons other than the controller from **attributing the personal data to an identified or identifiable natural person** ~~identifying a data subject, in such a way that, for them, the data subject is not or is no longer identifiable~~. NL (Comments): NL proposes to bring the description of pseudonymisation into line with that in the definition of pseudonymisation from the current Article 4(5), ending: "(…) *technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*".

Commission proposal	Drafting suggestions and Comments
	EE (Comments): Estonia supports the amendment. AT (Comments): • AT is open to further pursuing this proposal. • However, the provision should be move to Article 70 (see comment on Article 35(4) above). CZ (Drafting suggestions): (2) **For the purpose of paragraph 1 the Commission ~~The Board~~ shall ~~issue an opionion, in accordance with Article 64(2) of this Regulation, addressing~~ adopt implementing acts to address the application of pseudonymisation and anonymisation, including related technical and organisational measures, and specifying means and criteria to determine whether the application of pseudonymisation to personal data may, taking into account the costs, amount of time required, available technology, legal powers and restrictions and other relevant objective factors, effectively prevent persons other than the controller from identifying a data subject, in such a way that, for them, the data subject is not or is no longer identifiable.** CZ (Comments): CZ **red line:** Rules of such significance should be adopted in a binding, formal and predictable way. Mere opinion of EDPB is not acceptable and standard comitology is much preferred.

Commission proposal	Drafting suggestions and Comments
	In addition, given the importance of defining conditions when personal data cease to be, at least for some controllers, personal in nature, CZ believes that this Article should, at the very least, include the core requirements on the likelihood of preventing identification of a data subject. Proper procedure referred to in Art. 93(2) GDPR should be used. Given requirements of the industry and economic actors for legally sound de-personalisation of various data that are, in many contexts, simply not processed to be connected with identified individual, time is of the essence and a deadline of 12 months should be imposed.
~~(a) assess the state of the art of available techniques;~~	EE (Comments): Estonia supports the deletion.
~~(b) develop criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical recipients of data.~~	EE (Comments): Estonia supports the deletion.
(3) The ~~implementation~~ **Chair** of the ~~means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects~~ **Board shall request the opinion referred to in paragraph 1 no later than 12 months after the entry into force of this Regulation. The opinion shall be reviewed and updated where necessary**.	FR (Drafting suggestions): (3) The ~~implementation~~***Chair*** of the ~~means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects~~***Board shall request the opinion referred to in paragraph 1 by*** **[OP date = 2 months of the entry into application of this Regulation]** ***after the entry into force of this Regulation. The opinion shall be reviewed and updated where necessary***. FR (Comments): Comme indiqué précédemment, les autorités françaises sont favorables à conserver le délai initial prévu pour l'adoption de ces précisions.

Commission proposal	Drafting suggestions and Comments
	EE (Comments): Estonia supports the amendment. AT (Drafting suggestions): (3) The ~~implementation~~ Chair of the ~~means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects~~ Board shall request the opinion referred to in paragraph **2** no later than 12 months after the entry into force of this Regulation. The opinion shall be reviewed and updated where necessary. AT (Comments): There appears to be an error, the paragraph should refer to "opinion referred to in **paragraph 2**" not paragraph 1. CZ (Drafting suggestions): ~~(3) The implementation **Chair** of the means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects **Board shall request the opinion referred to in paragraph 1 no later than 12 months after the entry into force of this Regulation. The opinion shall be reviewed and updated where necessary.**~~ CZ (Comments): CZ believes that, while this obligation of the EDPB Chair is not contrary to GDPR, it illustrates rather clearly non-systemic nature of the proposal to replace standard comitology with soft law EDPB opinions. This system is does not really create obligations as regards both procedure and the outcome.

Commission proposal	Drafting suggestions and Comments
~~(4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.~~	EE (Comments): Estonia supports the deletion. CZ (Drafting suggestions): **(4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.**
~~(5) The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3).'~~	EE (Comments): Estonia supports the deletion. CZ (Drafting suggestions): (5) The Implementing Acts shall be adopted **no later than 12 months after the entry into force of this Regulation** in accordance with the examination procedure referred to in Article 93(~~3~~ **2**).' CZ (Comments): CZ strongly prefers, in this case, implementing acts to seeking new, non-systemic paths. However, proper procedure is referred to in Art. 93(2) GDPR. Given requirements of the industry and economic actors for legally sound de-personalisation of various data that are, in many contexts, simply not processed to be connected with identified individual, time is of the essence.
11. ~~In~~ Article ~~57(1)~~**57** is amended as follows:	EE (Comments):

Commission proposal	Drafting suggestions and Comments
	Estonia supports the amendment. AT (Comments): AT **supports the deletion** of the previously proposed paragraph (aa) and thanks the Presidency for the consideration. CZ (Comments): CZ strongly supports ES proposal on tax information exchange. While CZ is flexible, it prefers Option 1, preferably without bracketed second new subparagraph, which is not usual in tax cooperation, could be difficult to implement and involves potentially large administrative burden. BE (Comments): We preferred the harmonisation of article 57 rather than the recital in 40a. Preference to keep it in the operative text.art
(a) **in paragraph 1,** point (k) is deleted;	EE (Comments): Estonia supports the amendment.
(ab) paragraph 4 is replaced by the following; **'4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character or where an abusive intention on the part of the data subject submitting those requests can be demonstrated, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall, in the light of all the relevant circumstances of the case, bear the burden of demonstrating the manifestly unfounded or excessive character of the request.'**	EE (Comments): Estonia supports the amendment. AT (Comments): • AT **continues to support** the proposed amendment. FI (Comments):

Commission proposal	Drafting suggestions and Comments
	FI can support this proposal. CZ (Drafting suggestions): **(ab) paragraph 4 is replaced by the following;** **'4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character or ~~where an abusive intention on the part of the data subject submitting those requests can be demonstrated~~ because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their rights, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall, in the light of all the relevant circumstances of the case, bear the burden of demonstrating that the request is ~~the~~ manifestly unfounded or that there are reasonable grounds to believe that it is excessive ~~character of the request~~.'** SE (Comments): No comments. PL (Comments): We note that the issue of consistency between national supervisory authorities' guidance and EDPB guidance has been moved from the operative provisions to Recital 40a. While this reflects the importance of coherent application of the GDPR, it provides a more limited legal effect than an explicit provision in the Regulation itself. As regards Article 57(4), we support the proposed amendment, which may contribute to a more efficient use of supervisory authorities' resources and

Commission proposal	Drafting suggestions and Comments
	facilitate the handling of manifestly unfounded, excessive or abusive requests.
12. In Article 64(1), point (a) is deleted.	FR (Drafting suggestions): **12a. Article 64 is amended as follows:** **(a) the following paragraph is added:** **'2a. Controllers subject to this Regulation may present a reasoned request that any matter of consistent application directly relevant for them in more than one Member State be examined by the Board with a view to obtaining an opinion on this matter.'** **(b) paragraph 3 and 4 are replaced by the following:** **'3. In the cases referred to in paragraphs 1, 2 and 2a, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.** **12b. In Article 65(1), point (c) is replaced by the following:** **'(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not**

Commission proposal	Drafting suggestions and Comments
	follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned, the Commission or any controller concerned where that opinion was issued on the grounds of a request under Article 64(2a) or of Article 4129a may communicate the matter to the Board.' FR (Comments): Les autorités françaises rappellent leur proposition que les opérateurs puissent solliciter le CEPD pour lui demander un avis. Elles soulignent l'importance que figurent également dans l'omnibus numérique des mesures concrètes à destination des opérateurs économiques tendant à l'homogénéisation de l'interprétation du RGPD au sein du marché intérieur. A ce titre, les autorités françaises rappellent qu'elles ont proposé la création d'un mécanisme permettant aux opérateurs de solliciter l'adoption d'un avis par le CEPD à l'article 64 lorsqu'ils constatent des divergences d'interprétation impactant leurs activités transfrontalières. Ce dispositif répondrait directement aux besoins remontés par les acteurs économiques tout en renforçant la cohérence globale du cadre réglementaire. Les autorités françaises sont attachées à l'intégration dans la partie opérative du texte d'une disposition à destination des opérateurs permettant une application plus cohérente du RGPD. Cette proposition, en synergie avec le nouveau considérant 40a, apporterait une réponse équilibrée aux besoins des opérateurs sans compromettre le haut niveau de protection des données du RGPD. Les autorités françaises estiment que l'absence d'intégration de ses propositions à l'article 64 affaiblirait la portée globale du dispositif.
(12a) In Article 70(1), point (f) is amended as follows:	
(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the	EE (Comments): Estonia supports the amendment.

Commission proposal	Drafting suggestions and Comments
criteria and conditions for decisions based on profiling pursuant to Article 22(1);	AT (Comments): AT **is open** to further pursuing this amendment. FI (Comments): FI can support this proposal.
13. In Article 70(1), point (h) is deleted.	FR (Drafting suggestions): **13a. In Article 70(1), point (t) is replaced with the following:** **'(c) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and (2a), and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;'** FR (Comments): Cet amendement actualise le point correspondant des missions du Conseil afin de tenir compte des modifications proposées aux articles 64 et 65.
14. In Article 70(1), the following points are inserted:	FR (Drafting suggestions): **In Article 70(1), point (he) is added:** **'(he) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the appropriate technical and organisational measures to ensure a level of security appropriate to the level of risk pursuant to Article 32(5);'**

Commission proposal	Drafting suggestions and Comments
	FR (Comments): Cet amendement actualise la liste des missions du Conseil à la suite de la proposition d'amendement visant à introduire un paragraphe 5 à l'article 32, qui charge le Conseil d'adopter des lignes directrices précisant davantage les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au niveau de risque.
‘(ha) ~~prepare and transmit to the Commission a proposal for~~ **establish** a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and for which no data protection impact assessment is required, pursuant to Article 35.	EE (Comments): Estonia supports the amendment. FI (Comments): FI can support this proposal.
(hb) ~~prepare and transmit to the Commission a proposal for~~ **establish** a common template and a common methodology for conducting data protection impact assessments, pursuant to Article 35.	EE (Comments): Estonia supports the amendment. FI (Comments): FI can support this proposal.
(hc) ~~prepare and transmit to the Commission a proposal for~~ **establish** a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person pursuant to Article 33 **and a list of the circumstances in which it is not likely to result in such a high risk.**	EE (Comments): Estonia supports the amendment. FI (Comments): FI can support this proposal.

Commission proposal	Drafting suggestions and Comments
(hca) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the appropriate technical and organisational measures to ensure a level of security appropriate to the level of risk pursuant to Article 32.	EE (Comments): Estonia supports the amendment. AT (Comments): AT **supports** the proposal to issue EDPB guidelines, recommendations and best practices regarding data security measures. MT (Comments): See the comment on recital 27a and Article 29a. Our preference would be for guidelines specifically on pseudonymisation, but broader guidelines on "*the appropriate technical and organisational measures to ensure a level of security appropriate to the level of risk pursuant to Article 32"* would be beneficial. FI (Comments): FI can support this proposal. CZ (Drafting suggestions): ~~**(hca) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the appropriate technical and organisational measures to ensure a level of security appropriate to the level of risk pursuant to Article 32.**~~ CZ (Comments):

Commission proposal	Drafting suggestions and Comments
	CZ cannot support the insertion of this point, because it constitutes a new and substantial mandate not foreseen in GDPR and lacking justification or impact assessment. The proposal appears to reinterpret Article 32(1), which was intentionally left open by the legislator, thereby risking over-specification and reduced flexibility. It has a potential to impose further administrative and financial burden on each and every controller. Moreover, such soft law related security is not coordinated with cyber security bodies. Rather than simplifying compliance, the measure risks increasing complexity and creating further pressure for additional soft law instruments, without a consistent approach across related provisions (e.g. Articles 24 and 25) or areas.
(hcb) issue the opinion on the application of pseudonymisation and anonymisation referred to in Article 29a.'	EE (Comments): Estonia supports the amendment. MT (Comments): See the comment on recital 27a and Article 29a. FI (Comments): FI can support this proposal. SK (Comments): **SK:** We propose to delete this provision. An explanation is provided in the comments to Article 29a.
15. After Article ~~88~~**8**, the following ~~articles are~~ **article is** added:	FR (Comments):

Commission proposal	Drafting suggestions and Comments
	Les autorités françaises restent opposées à l'introduction de cette disposition sans analyse d'impact plus étayée et travail plus approfondi autour des enjeux et des solutions techniques et juridiques proposées ici. En l'état, malgré le soutien qu'elles apportent à l'objectif louable de faciliter le consentement pour les personnes concernées, et en dépit des efforts de la Présidence, la disposition continue de soulever trop d'interrogations et de difficultés (renforcement de la position dominante des « gatekeepers » au sens du DMA, difficultés d'identification des « médias » bénéficiaires de l'exemption, coût économique pour les acteurs y compris pour la presse) pour être introduite dans un omnibus. Par définition, les discussions sur ce texte doivent porter sur des amendements ciblés et efficaces pour alléger la charge des opérateurs. Sur le sujet du consentement centralisé, l'objectif ne paraît pas pouvoir être atteint ni de manière simple et ciblée, ni dans le délai qu'impliquent les travaux sur un omnibus. Les autorités françaises prennent des solutions alternatives évoquées par la Commission pour enregistrer les préférences, mais rappelle que les navigateurs ont naturellement vocation à accueillir ces dernières au vu de leur taux d'utilisation d'où un risque accru de conforter des acteurs déjà en position dominante si le consentement centralisé est imposé en l'état (Chrome et Safari représentent 79% du trafic européen en matière de recherche internet - Statcounter, Browser Market Share Europe, March 2026). Enfin, les autorités françaises soulignent que l'ajout suivant l'interdiction faite aux fournisseurs de navigateurs et/ou autres types de terminaux d'utiliser les préférences des utilisateurs à d'autres fins que celle prévue par l'article est dépourvue d'effectivité faute de précisions sur le mécanisme utilisé dans ce cadre. Les autorités françaises réitèrent leur demande de supprimer cette disposition, ainsi que des définitions et considérants correspondants. CZ (Comments): CZ is flexible regarding the deletion of Article 88c or a possible shift of its substance into a recital. (At the same time, CZ strongly opposes the wording in Recital 33a requiring controllers to choose the "most" appropriate legal basis. The controller is responsible for having appropriate legal ground or grounds for processing,

Commission proposal	Drafting suggestions and Comments
	but choosing "the most" appropriate one goes above the GDPR and would create unnecessary legal uncertainty and complication rather than simplification.)
~~'Article 88a~~	EE (Comments): Estonia supports the deletion.
~~Processing of personal data in the terminal equipment of natural persons~~	
~~(1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.~~	
~~(2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1).~~	
~~(3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following:~~	
~~(a) carrying out the transmission of an electronic communication over an electronic communications network;~~	
~~(b) providing a service explicitly requested by the data subject;~~	
~~(c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;~~	

Commission proposal	Drafting suggestions and Comments
~~(d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.~~	
~~(4)~~	
~~Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:~~	
~~(a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;~~	
~~(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;~~	
~~(c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.~~	
~~This paragraph also applies to the subsequent processing of personal data based on consent.~~	
~~(5) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]~~	
Article ~~88b~~**8a**	NL (Comments): Other than the amendments included below, the Netherlands supports this article, specifically with the aim of reducing consent fatigue and regulatory burden for businesses having to set up compliant cookie banners, and would

Commission proposal	Drafting suggestions and Comments
	like to emphasise that we are in favour of retaining this article in this proposal. FR (Drafting suggestions): ~~Article 88b~~**~~8a~~** FR (Comments): **Les autorités françaises réitèrent leur demande ferme de suppression de cet article.** Proposition visant à supprimer cette disposition, compte tenu des conséquences que la centralisation du consentement aurait sur l'écosystème médiatique, de son non-respect du RGPD et du renforcement de la position dominante des services intermédiaires que cela entraînerait. EE (Comments): Estonia is currently reviewing this amendment and intends to address the issue in Coreper. DK (Drafting suggestions): ~~Article 88b~~**~~8a~~** DK (Comments): DK is still very concerned about the uncertain effects and potentially far-reaching consequences of introducing the mechanism. The objective of the Digital Omnibus is to swiftly deliver simplification and reduce burdens without unintended consequences, and the process should not be delayed more than necessary. Introducing centralised consent would

Commission proposal	Drafting suggestions and Comments
	require further discussion and a better understanding of the practical implications, including a thorough impact assessment. DK is in favour of continued dialogue to explore other viable solutions to cookie-fatigue. We suggest to delete the Article altogether. MT (Comments): In our view, it might be preferable to have all provisions relating to termination equipment within the ePrivacy Directive. However, we have no strong objections to the suggested new article 8a, particularly the changes proposed in paragraphs 6 and 7a thereof. Should this new article 8a be maintained within the GDPR, then an amendment to Article 83(5) GDPR (fining powers for infringements) would be necessary to include a reference to this new article 8a. CZ (Drafting suggestions): **CZ could support deleting whole Article 8a** CZ (Comments): CZ: CZ welcomes efforts to simplify the EU's digital legislative framework and supports objectives aimed at reducing the administrative burden while maintaining a high level of protection for fundamental rights, particularly the protection of personal data. At the same time, however, we consider it essential that the proposed changes, concerning the cookies (moved to the ePrivacy part) and consent level browser (currently Art. 8a) are supported by a sufficiently detailed technical and impact analysis.

Commission proposal	Drafting suggestions and Comments
	Given the lack of data explaining the impact on different sectors and lacking the clear explanation from the EC (that we asked repeatedly) on how the proposed browser-level consent in Art. 8a would technically work, i.e. how the signal would be communicated between the different providers, and given that we are also opposing the broadened scope by addition of the operation systems, Czechia is having serious doubts of an added value of this part of the proposal, which is in our view against the principle of simplification. In this regard, Czechia can support its deletion. SI (Comments): We maintain a degree of reservation with regard to the proposed new Article 8a. The primary reason for this reservation is the lack of an impact assessment and the consequent absence of sufficient information, which gives rise to legal uncertainty as to the implications of such a provision. While the proposed measure may, in principle, be conducive to enhancing the user experience, its concrete effects on the protection of individuals' fundamental rights remain unclear. Likewise, the potential impact on economic operators within the Union has not been sufficiently substantiated. SE (Comments): Sweden refers to our additional comments, sent in on the 20th of May. To clarify: SE welcomes a removal of art. 88b.

Commission proposal	Drafting suggestions and Comments
	Centralised consent and its potential implications remain difficult to assess. The objective of the Digital Omnibus is to swiftly deliver simplification without unintended consequences, and the process should not be delayed more than necessary. Introducing centralised consent would require further discussion and a better understanding of the practical implications. Furthermore, as previously stressed, we are concerned about the practical implications thereof, e.g. with regards to the risk of market concentration to a few platform operators which could result in distortion of competition, as well as the consequences for certain actors, such as media service providers. SE is in favour of continued dialogue to explore other viable solutions to cookie-fatigue. While SE appreciates that the proposal included an exemption for media services, there are concerns about the operationalization of it. PL (Drafting suggestions): Delete article 8a. In case this provision is to be retained, we maintain our previous drafting suggestion to transfer Article 8a in its entirety to Article 5 of Directive 2002/58/EC. PL (Comments): Given the number of uncertainties surrounding this provision, it would be reasonable to halt work on the proposal within the Digital Omnibus and to recommence it under a different legislative act following a thorough analysis of its impact on the EU economy.

Commission proposal	Drafting suggestions and Comments
	However, if this provision is to be retained, we propose to transfer it to Directive 2002/58/EC. The proposed changes to the law on the protection of end-users' personal data, as set out in the draft Digital Omnibus, effectively create two parallel legal systems. The reducing consent fatigue through automated and machine-readable consent signals would be more appropriately regulated within the framework of Directive 2002/58/EC.
Consent through automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons	NL (Drafting suggestions): **Consent through** automated and machine-readable indications of data subject's choices with respect to ~~**processing of personal data in the**~~ terminal equipment ~~**of natural persons**~~ LU (Comments): We reiterate our overall support for the objective of improving user experience and enhancing provider compliance by significantly reducing the prevalence of cookie banners on online interfaces. Overall, we believe it is important to discuss, at EU level, solutions like Article 88b GDPR, which sets out requirements for automated and machine-readable indications of data subjects' choices. We nevertheless recognise both the significant implications of any modification to the "cookies" regime and the inherently technical and complex nature of assessing its practical and economic impact. We therefore align with other Member States which - while not opposing the principle of this change - consider that is would benefit from a thorough and well-substantiated impact assessment.

Commission proposal	Drafting suggestions and Comments
	We support continuing meaningful, evidence-based discussions on this provision outside the scope of the current Digital Omnibus process, which presents inherent constraints for addressing such a technically complex topic. FR (Drafting suggestions): ~~**Consent through** automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons~~ DK (Drafting suggestions): ~~**Consent through** automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons~~ PL (Comments): Due to proposed provision 8a as part of the GDPR and the transfer of 88a to the Directive 2002/58/EC, there is a lack of clear guidance on the relationship between consent (from the article 8a) and the exceptions set out in the Directive 2002/58/EC regarding the requirement to obtain consent. To reiterate our earlier comments, it is necessary to harmonise the regulatory approach to cookies and other tracking technologies through the unambiguous categorisation of cookies and similar technologies (e.g. in the form of the guidelines), with particular regard to those strictly necessary for the operation or provision of a service requested by the user, including files used for purely analytical purposes of the first-party and those serving to enhance security or prevent fraudulent activities, and to clearly explain how compliance with this provision interacts with the exceptions set out in art. 5(3) of Directive 2002/58/EC. ES

Commission proposal	Drafting suggestions and Comments
	(Comments): ES: Scrutiny reservation
(1) **For the purpose of data subject consent to the storing of personal data, or gaining of access to personal data already stored in the terminal equipment of a natural person in accordance with Directive 2002/58/EC,** controllers shall ensure that their online interfaces allow data subjects to:	NL (Drafting suggestions): (1) **For the purposes of granting, refusing or withdrawing ~~data subject~~ consent ~~to the storing of personal data, or gaining of access to personal data already stored in the terminal equipment of a natural person~~ in accordance with article 5(3) of Directive 2002/58/EC,** controllers shall ensure that their online interfaces allow data subjects to: NL (Comments): The proposed article 8a GDPR is limited to *personal* data, while article 5, paragraph 3 of the ePrivacy-directive is applicable to *all information* stored in terminal equipment. To further improve the effective application of this article and prevent legal uncertainty, it is important to further align this article 8a to correspond with the ePrivacy-directive. Alternatively, this article could also be expanded to *information* in general to match the scope of article 5, paragraph 3 of the ePrivacy-directive. However, we question whether this is consistent with the scope of the GDPR. IT (Drafting suggestions): **Articolo 88b** **We propose that the provision be deleted or reformulated.** In case it is maintained, the following modification is proposed: *For the purpose of **identified** data subject consent to the storing of personal data, or gaining of access to personal data already stored in the terminal*

Commission proposal	Drafting suggestions and Comments
	*equipment of **an identified** natural person in accordance with Directive 2002/58/EC, controllers shall ensure that their online interfaces allow data subjects to: …* IT (Comments): Article 88b We propose deleting or reformulating this provision. The problem with the current wording lies in its lack of a clear distinction between identified users and those browsing anonymously or otherwise not personally identified. In the former case (in which users are identified because they have registered on a site or provided other information by filling out a form), there is also the issue of privacy protection as well as the processing of personal data in relation to the use of cookies. In the latter case, however, this does not apply because the user is anonymous, and therefore there can be no violation of privacy, let alone the GDPR, because no personal data is involved. It is true that the provision uses the GDPR's own notion of "data subjects," thus implying that the scope of application is limited to actually identified users, but this is not clearly expressed. The reason why Article 88b should be deleted is that, for the reasons and within the limits outlined above, it is impossible, as it is worded, to demonstrate that a specific, unidentified user has actually given consent. Therefore, if the obligation were to remain in force, it would impose technical and organizational burdens disproportionate to the regulatory rationale because it would also apply to individuals who do not fall within the scope of protection. Alternatively, opting to retain the provision would explicitly exclude the applicability of the article to anonymous users, with wording such as the following, which limits its application to only truly identified users FR

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): ~~(1) **For the purpose of data subject consent to the storing of personal data, or gaining of access to personal data already stored in the terminal equipment of a natural person in accordance with Directive 2002/58/EC,** controllers shall ensure that their online interfaces allow data subjects to:~~ DK (Drafting suggestions): ~~(1) **For the purpose of data subject consent to the storing of personal data, or gaining of access to personal data already stored in the terminal equipment of a natural person in accordance with Directive 2002/58/EC,** controllers shall ensure that their online interfaces allow data subjects to:~~
(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;	NL (Drafting suggestions): (a) Give consent **for specific categories of purposes** through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled; NL (Comments): NL proposes to reintroduce the phrase "for specific categories of purposes" because of the requirement of *specific* consent under Art. 7 GDPR. FR (Drafting suggestions): ~~(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;~~ DK (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;~~ PL (Comments): It is unclear why the 'for specific categories of purposes' provision, which would have allowed users to specify the type of processing to which they consent, and was included in the previous version, was removed.
(b) ~~decline~~**refuse** a request for consent ~~and~~**or** exercise the right to object pursuant to Article 21(2) through automated and machine-readable means;	HR (Drafting suggestions): (~~(b) decline~~**refuse** ~~a request for consent and~~**or** ~~exercise the right to object pursuant to Article 21(2) through automated and machine-readable means;~~ FR (Drafting suggestions): ~~(b) decline~~**refuse** ~~a request for consent and~~**or** ~~exercise the right to object pursuant to Article 21(2) through automated and machine-readable means;~~ DK (Drafting suggestions): ~~(b) decline~~**refuse** ~~a request for consent and~~**or** ~~exercise the right to object pursuant to Article 21(2) through automated and machine-readable means;~~
(ba) withdraw consent through automated and machine-readable means.	NL (Comments): NL thanks the Presidency for the addition of subparagraph ba. FR (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~**(ba) withdraw consent through automated and machine-readable means.**~~ DK (Drafting suggestions): ~~**(ba) withdraw consent through automated and machine-readable means.**~~ HU (Comments):
	HU: We positively note the Presidency's approach regarding Article 8a para 1 new point (ba), which aims to ensure granular and informed consent mechanisms in line with GDPR principles and effective user control over consent preferences by intruducing the possibility to withdraw consent through automated and machine readable means.
	PL (Comments): If article 8a is to stay, it's reasonable to include this provision (ba). Furthermore, it is essential to guarantee users a genuine right to decide the scope within which they give or refuse consent for specific entities to access their data. In this regard, it would be also reasonable to maintain the addition of recital 46a, whilst pointing out that it is necessary to provide for a provision that would allow users to specify exceptions to their general consent or refusal of consent for websites of their choice or at least expand recital 46a in this regard.
(2) Controllers shall respect **automated and machine-readable means expressing** the choices made by data subjects in accordance with paragraph 1.	HR (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~(2) Controllers shall respect **automated and machine-readable means expressing** the choices made by data subjects in accordance with paragraph 1.~~ FR (Drafting suggestions): ~~(2) Controllers shall respect **automated and machine-readable means expressing** the choices made by data subjects in accordance with paragraph 1.~~ DK (Drafting suggestions): ~~(2) Controllers shall respect **automated and machine-readable means expressing** the choices made by data subjects in accordance with paragraph 1.~~
(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.	NL (Comments): The NL maintains its study reservation regarding the exception for media service providers in Article 8a(3). On the one hand, the media hold a special position regarding freedom of information, as guaranteed in Article 10 of the ECHR. On the other hand, sectoral carve-outs accepted in a fundamental rights law must be avoided. Furthermore, NL has concerns regarding the operationalisation of this exemption in practice and the persistence of cookie fatigue because of this exception. IT (Comments): Non-applicability of the "media exemption" to audience measurement: The current wording of Article 8a provides that "media service providers" are exempt from the centralized collection of consent via the browser (or operating system) for the management of cookies and/or other tracking tools (as referred

Commission proposal	Drafting suggestions and Comments
	to in paragraphs 1 and 2 of that article) and may nevertheless request direct consent for advertising and profiling purposes. However, this provision classifies such media service providers as "data controllers" (within the meaning of Article 4(1)(7) of the GDPR). It follows that the exemption applies exclusively to processing operations in which such entities actually act as data controllers, such as technical cookies used to maintain an active login or browsing session or to store user preferences, such as language. The exemption would not, however, apply to all tracking activities in which the data controller is a party other than the media service provider, i.e., to most of the cases that are actually relevant in the sector. The current wording of the proposal therefore appears excessively restrictive and rigid, with the risk of excluding, from the scope of the exemption, the measurement activities carried out by third parties acting on behalf of the media industry. For these reasons, to protect and promote the independent measurement activities conducted by JICs, the exemption should apply to the measurement of the audience of an online service in cases where such activity is carried out (i) directly by the data controller of the online service, for its own purposes; or (ii) by collective bodies responsible for official audience measurement or by third parties appointed by the owners of digital services. FR (Drafting suggestions): ~~(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.~~ DK (Drafting suggestions): ~~(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.~~ LV

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service, **nor shall it apply to either processors or independent audience measurement providers, in each case acting on behalf of such media service providers, to the extent strictly necessary for the provision, measurement or monetisation of the media service.** LV (Comments): With reference to the corrections made to the recital 44 and in order to ensure legal certainty and prevent tech platforms from blocking these essential tools at the browser level, we believe this intent must be mirrored also in Article 8a(3). In our view, aligning the operative text with the recital is the only way to safeguard media sustainability, prevent platform dominance and ensure this exemption actually works on the ground.
(4) The Commission shall~~, in accordance with Article 10(1) of Regulation (EU) 1025/2012,~~ request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices**, subject to consultation, in accordance with Article 10 of Regulation (EU) 1025/2012**.	FR (Drafting suggestions): ~~(4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices, subject to consultation, in accordance with Article 10 of Regulation (EU) 1025/2012.~~ EE (Comments): We propose to fix a deadline for standards. DK

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): ~~(4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices~~**~~, subject to consultation, in accordance with Article 10 of Regulation (EU) 1025/2012~~**~~.~~
Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1.	FR (Drafting suggestions): ~~Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1.~~ DK (Drafting suggestions): ~~Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1.~~
(5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].	FR (Drafting suggestions): ~~(5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].~~ DK (Drafting suggestions): ~~(5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].~~

Commission proposal	Drafting suggestions and Comments
(6) Providers of web browsers~~, which are not SMEs,~~ **and providers of operating systems of terminal equipment in relation to software applications operating on that terminal equipment** shall provide the technical means to allow data subjects to give their consent**, to withdraw consent,** and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to ~~5~~**4** of this Article.	NL (Comments): NL thanks the Presidency for adding the withdrawal of consent to this paragraph. FR (Drafting suggestions): ~~(6) Providers of web browsers, which are not SMEs,~~ ~~**and providers of operating systems of terminal equipment in relation to software applications operating on that terminal equipment**~~ ~~shall provide the technical means to allow data subjects to give their consent~~~~**, to withdraw consent,**~~ ~~and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5~~**4**~~ of this Article.~~ DK (Drafting suggestions): ~~(6) Providers of web browsers, which are not SMEs,~~ ~~**and providers of operating systems of terminal equipment in relation to software applications operating on that terminal equipment**~~ ~~shall provide the technical means to allow data subjects to give their consent~~~~**, to withdraw consent,**~~ ~~and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5~~**4**~~ of this Article.~~
(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].	FR (Drafting suggestions): ~~(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].~~

Commission proposal	Drafting suggestions and Comments
	DK (Drafting suggestions): ~~(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].~~
7a. Providers of web browsers and providers of operating systems of terminal equipment in relation to software applications operating on that terminal equipment shall not process the data subject's choices referred to in paragraph 1 for any other purpose than transmitting the signal to providers of online interfaces.	NL (Drafting suggestions): 7a. Providers of web browsers and providers of operating systems of terminal equipment in relation to software applications operating on that terminal equipment shall not process the data subject's choices referred to in paragraph 1 for any other purpose than transmitting the signal to providers of online interfaces. **Article 83 applies accordingly to web browsers and other providers of operating systems of terminal equipment in relation to software applications operating on that terminal equipment who infringe this obligation, subject to the applicability of the maximum administrative fine referred to in Article 83, paragraph 5.** NL (Comments): For reasons of legal certainty, NL proposes to add the threat of administrative fines for this new obligation, because this seems not to be covered by the current Article 83. For a further explanation, we refer to our amendment to Article 83 on the previous compromise text. FR (Drafting suggestions): ~~**7a. Providers of web browsers and providers of operating systems of terminal equipment in relation to software applications operating on that terminal equipment shall not process the data subject's choices**~~

Commission proposal	Drafting suggestions and Comments
	~~**referred to in paragraph 1 for any other purpose than transmitting the signal to providers of online interfaces.**~~ DK (Drafting suggestions): ~~**7a. Providers of web browsers and providers of operating systems of terminal equipment in relation to software applications operating on that terminal equipment shall not process the data subject's choices referred to in paragraph 1 for any other purpose than transmitting the signal to providers of online interfaces.**~~
~~Article 88c~~	EE (Comments): Estonia supports the deletion. AT (Comments): AT **can support** the deletion of Article 88c. SK (Comments): **SK:** We support deletion of this article.
~~Processing in the context of the development and operation of AI~~	
~~Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights~~	

Commission proposal	Drafting suggestions and Comments
~~and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.~~	
~~Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'~~	
(...)	
Article 5 **Amendments to and Directive 2002/58/EC (ePrivacy Directive)**	EE (Comments): Estonia is currently reviewing this amendment and intends to address the issue in Coreper. ES (Comments): ES: Scrutiny reservation
Directive 2002/58/EC is amended as follows:	
1. Article 4 is deleted;	SI (Comments): Republic of Slovenia opposes the repeal of Article 4 of Directive 2002/58/EC, as this would mean a reduction in regulation in the field of security of electronic communications services. The security of processing should remain regulated within the framework of the protection of privacy in electronic communications.

Commission proposal	Drafting suggestions and Comments
2. ~~After~~**In** Article ~~5(3)~~**5**, **paragraph 3 is replaced by** the following subparagraph ~~is added~~:	LU (Comments): We remain sceptical about the proposal to maintain and amend Article 5(3) of the ePrivacy Directive to introduce additional consent exceptions. Simplification also requires consolidation of legal frameworks, and our understanding is that keeping this provision within the ePrivacy Directive - rather than integrating it into the GDPR - would ultimately undermine this objective. HU (Comments): HU: We welcome the Presidency's decision to remove 'contextual advertising' from the scope of the proposed consent exemptions under Article 5(3) ePrivacy, which contributes to greater legal clarity and better preserves the balance between simplification and the protection of users' rights. FI (Comments): FI remains concerned about the proposal's impacts on the vital role of digital advertising in the media sector. Therefore, FI repeats its previous proposal concerning media sector. SE (Comments): Regarding this matter, Sweden supports the Polish non-paper.
~~'This paragraph~~**3. Member States** shall ~~not apply if the~~ **ensure that the storing of information, or gaining of access to information already stored, in the terminal equipment of a** subscriber or user is **only allowed when that person has given his or her consent, in accordance with Regulation (EU) 2016/679.**	HR (Drafting suggestions): ~~paragraph~~**3. Member States** shall ~~not apply if the~~ **ensure that the storing of information, or gaining of access to information already stored, in the terminal equipment of a** subscriber or user is **only allowed when that**

Commission proposal	Drafting suggestions and Comments
Storing of information, or gaining of access to information already stored, in the terminal equipment of a natural person **without consent, and subsequent processing for the same purpose, shall be lawful to the extent it is strictly necessary for any of the following purposes:**	**person has given his or her consent, in accordance with Regulation (EU) 2016/679.** **Storing of information, or gaining of access to information already stored, in the terminal equipment of** a natural person **without consent, ~~and subsequent processing for the same purpose~~, shall be lawful to the extent it is strictly necessary for any of the following purposes:** HR (Comments): We suggest to delete wording marked in red because, in our view, considering it relates to the same purpose, is redundant. FR (Comments): MT (Comments): We agree with the Presidency's approach of streamlining the wording with already existing ePrivacy terminology. We further thank the Presidency for delimiting the processing to what is "*strictly"* necessary in Article 5(3) of the ePrivacy Directive. SI (Comments): Slovenia welcomes the new list of exceptions. However, regarding the fourth exception, this should only be allowed to the extend that security updates are discretely packaged and do not in any way change the functionality of the software on the terminal equipment (including the interaction with other software od setting chosen by the user. PL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): ~~'This paragraph~~3. **Member States** shall ~~not apply if the~~ **ensure that the storing of information, or gaining of access to information already stored, in the terminal equipment of a** subscriber or user is **only allowed when that person has given his or her consent, in accordance with Regulation (EU) 2016/679.** **Storing of information, or gaining of access to information already stored, in the terminal equipment of** ~~a natural person~~ **a subscriber or user without consent, and subsequent processing for the same purpose, shall be lawful to the extent it is strictly necessary for any of the following purposes:** PL (Comments): It is unclear why the reference to 'natural person' was changed to 'subscriber or user' only in the first sentence, whilst the reference to 'natural person' was retained in the second sentence. This should be harmonised, by changing "natural person" to "subscriber or user", particularly as the provision refers to a 'user' after listing the exceptions.
a) carrying out the transmission of an electronic communication over an electronic communications network;	
b) providing a service explicitly requested by the user;	NL (Drafting suggestions): b) providing **an information society service** ~~a service~~ explicitly requested by the **subscriber or** user; NL (Comments):

Commission proposal	Drafting suggestions and Comments
	In the absence of a justification for extending "information society service" to "service", and the as yet unknown consequences of this extension, NL prefers to leave the text of this element from the current Article 5(3) of the e-Privacy Directive unchanged. Furthermore, it seems necessary to add the "subscriber" (in addition to "the user") because of the e-Privacy Directive terminology. This last remark also applies to subparagraphs c and d. PL (Drafting suggestions): b) providing a service explicitly requested by the user **and improving functionality of the requested service;**
c) creating anonymous aggregated~~, and the~~ information ~~stored or accessed constitutes or leads to the processing~~ **about the usage of an online service requested by the user to measure the audience of such a service, where it is carried out by the provider of that online service, or by a third party acting together with or on behalf of this provider, solely for their own use, including where the third party is performing audience measurement in accordance with Article 24 of Regulation (EU) 2024/1083;**	IT (Drafting suggestions): c) creating anonymous ~~aggregated, and the~~ information ~~stored or accessed constitutes or leads to the processing~~ about the usage of an online service requested by the user to measure the audience of such a service, where it is carried out by the provider of that online service, ~~or~~ by a third party acting together with or on behalf of this provider, solely for their own use, or by an entitled and independent ~~including where the~~ third party ~~is~~ performing audience measurement in accordance with Article 24 of Regulation (EU) 2024/1083; IT (Comments): This amendment aims at including the performance of audience measurement as defined in Regulation (EU) 2024/1083 for instance when it is performed by an entitled and independent third party acting as independent data controller jointly authorized by advertisers and publishers, solely for the measurement of the overall market performance such as Joint Industry Committees which play a critical role in ensuring transparency, comparability, and credibility of audience information across the market

Commission proposal	Drafting suggestions and Comments
	FR (Drafting suggestions): **<u>Measuring the audience of an online service in order to create anonymous aggregated information about the usage of an online service, where it is carried out by the provider of that online service, or jointly with a third party acting as a controller,</u> including where the third party is performing audience measurement in accordance with article 24 of Regulation (EU) 2024/1083;** FR (Comments): **Les autorités françaises restent réservées sur les amendements apportés au point c) du paragraphe 2 en matière de mesure d'audience dans la mesure où il semble que la mesure d'audience au titre de l'article 24 du Règlement EMFA ne s'effectue précisément pas pour le seul usage du fournisseur lui-même. En effet, dans le cadre de ces mesures d'audience tierces, l'objectif est de fournir une mesure d'audience à des tiers pour assurer la fourniture d'un service plus neutre. Il convient donc de mettre en cohérence l'Omnibus avec l'EMFA en supprimant la condition de consentement, superflue dans le cadre de cette exemption (« demandé par l'utilisateur ») et la restriction mise à l'utilisation des données « pour son propre usage ».** **En matière de publicité contextuelle, les autorités françaises sont favorables à toute mesure permettant de développer l'usage de la publicité contextuelle en complément de la publicité ciblée, notamment par le biais d'une exemption pour cette activité dans la directive ePrivacy.** Voir également le considérant 44. Correction apportée aux dispositions relatives aux étapes de collecte des données afin de refléter la réalité du processus de mesure d'audience. La modification porte également sur le rôle des tiers de confiance, dont la participation est essentielle, car sans eux, la mesure d'audience serait entièrement laissée à la discrétion des plateformes.

Commission proposal	Drafting suggestions and Comments
	DK (Drafting suggestions): **creating ~~anonymous~~ aggregated~~, and the~~** information ~~stored or accessed constitutes or leads to the processing~~ **about the usage of an online service requested by the user to measure the audience of such a service, where it is carried out by the provider of that online service, or by a third party acting together with or on behalf of this provider**, ~~**solely for their own use,**~~ **including where the third party is performing audience measurement in accordance with Article 24 of Regulation (EU) 2024/1083**; DK (Comments): We welcome the reference to EMFA, however, there are still challenges with the wording, which undermines the purpose of allowing media service providers to conduct audience measurement on the same terms as all other companies. We find it necessary to delete “anonymous” as well as “solely for their own use” in order to to ensure compatibility with EMFA. CZ (Drafting suggestions): After (c), the following points are added: **‘(ca) contextual advertising and related limitation of advertisement display, audience measurement and preventing fraudulent misrepresentation of audience, unless at least one of the following applies:**

Commission proposal	Drafting suggestions and Comments
	(i) the processing is likely to result in a risk to the rights and freedoms of natural persons; **(ii) the processing involves profiling;** **(iii) personal data are stored at the time when the electronic communication service is not actively used;** **(iv) personal data are connected with past or future activity of the data subject.** **(cb) other techniques similar to contextual advertising specified by means of implementing act of the Commission, unless at least one of the conditions referred to in points (e) (i) to (iv) applies.'** CZ (Comments): CZ: CZ suggests adding new exemptions concerning activities that are not based on profiling, i.e. covering low-risk to the rights and freedoms, non-profiling activities that do not involve any retention of personal data beyond the user's active session nor any link to past or future behaviour. This suggestion is inspired by the EDPB/EDPS joint opinion (point 104) which emphasises the need to create incentives to use less-intrusive forms of online advertising and aimed to make the rules more proportionate, i.e. allowing some forms of targeted advertising, which is crucial for European publishers and service providers. While we deem our suggestion proportionate, we are open to

Commission proposal	Drafting suggestions and Comments
	discuss it further. As stated in relation to rec. 44, addition of this text is not a red line for Czechia so far but we are convinced that the final text should appropriately balance the data protection and industrial needs. In this regard, we consider this addition as very important. CZ considers it also important that the GDPR allows the Commission to specify through implementing acts, while preserving Member States' control through comitology, other technical modalities than contextual advertising – that are similarly low-risk - to make the provision future proof and to prevent the long-term legislative deadlock phase. The EDPB should be closely involved in the whole process of drafting the acts. SE (Comments): SE
d) maintaining or restoring the security of the interface strictly necessary for the provision of an information society service requested by the user or the security of the terminal equipment used for the provision of such service, including in particular cybersecurity, the protection of personal data **and privacy of the user and prevention of fraud;**	NL (Comments): The Netherlands can support the inclusion of a security exception aimed at safeguarding the cybersecurity and protection of personal data of the user itself. However, the newly introduced expansion of this paragraph to include any and all fraud prevention measures makes this exception too broad and creates the risk of enabling various data processing applications that may be unintended or undesirable. In this broad formulation, and in the absence of an explanation of the necessity and meaning, we therefore suggest removing this new addition. If member states nevertheless want to proceed with a reference to fraud prevention, it should at least be strictly delineated of the specific processing permitted under this exception and an explanation should be given (in a recital). We make a study reservation for the review of such delineation and explanation.

Commission proposal	Drafting suggestions and Comments
	DK (Comments): DK questions the removal of the additional exception for the measuring of contextual advertising (the previous Article 5(3)(d)) which was an addition we saw merit in. Introducing exemptions for consent for harmless purposes is in our view a prudent way to reduce cookie fatigue and reduce burdens for companies. PL (Drafting suggestions): **d) maintaining, ~~or~~ restoring, or ensuring the security of the interface strictly necessary for the provision of an information society service requested by the user or the security of the terminal equipment used for the provision of such service, including in particular cybersecurity, the protection** of personal data **and privacy of the user and prevention of fraud and unauthorised access;** **(e) processing where the controller deploys recognised privacy-enhancing technologies (PETs) that effectively mitigate risks to the rights and freedoms of data subjects, in accordance with the technical specifications adopted pursuant to paragraph 4, 5 and 6.** **In Article 5, paragraph 4 is added:** **For the purpose of Article 5 paragraph (3)(e), the Commission shall:** **(a) assess the state of the art of available technologies;** **(b)develop criteria to assess the effectiveness of risk mitigation in relation to the specific** **categories of data and processing operations.** **In Article 5, paragraph 5 is added**

Commission proposal	Drafting suggestions and Comments
	(5) Article 5(3)(e) enters into force only 6 months after the adoption of relevant implementing acts by the European Commission. The implementing acts shall specify the technical standards and criteria to determine whether a technology qualifies as a recognised Privacy Enhancing Technology (PET) and effectively mitigates risks as referred to in paragraph 3(e). PL (Comments): We submit for consideration alternative options for enhancing the privacy of end-users of electronic communications services, for example through solutions collectively referred to as Privacy Enhancing Technologies (PET) – technical solutions, certified by independent bodies, that embed privacy directly into the architecture of data processing. Rather than preventing data use entirely, they can enable organisations to analyse, share and process data while minimising exposure of personal information and reducing re-identification risks. It is worth analyzing the interoperability and effectiveness of such tools used so far and the potential for their development, while respecting user privacy. To protect user interests, it is worth considering establishing a basis for issuing guidelines on PET by the European Commission in cooperation with European Data Protection Board, specifying the requirements they must meet.
The user shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means. If the user gives consent, the provider shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject. If the data subject refuses a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.	HR (Drafting suggestions): ***The user shall be able to refuse*** *or withdraw* ~~***requests for***~~ ***consent in an easy and intelligible manner with a single-click button or equivalent means. If the user gives consent, the provider shall not*** ~~***make a new***~~ ***request*** ~~***for***~~ ***new consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject*** ~~of personal data~~***. If the data subject***

Commission proposal	Drafting suggestions and Comments
	refuses ~~a request for~~ to give consent, the controller shall not ~~make a new~~ request ~~for~~ new consent for the same purpose for a period of at least six months. HR (Comments): In addition to the wording suggestions, considering text in this paragraph in the beginning refers to the consent in accordance with Regulation (EU) 2016/679, acknowledging this subparagraph further clarifies possible practical implications of the actions taken by the controller that relates to conditions for consent set in Art 7 of the GDPR, we suggest to move this subparagraph to the relevant provisions of the GDPR (possible in recital). FR (Drafting suggestions): ***The user shall be able to refuse requests for consent in an easy and intelligible manner ~~with a single-click button or equivalent means~~. If the user gives consent, the provider shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject ~~of personal data~~. If the data subject refuses a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least three months.*** FR (Comments): **Les autorités françaises restent réservées concernant la possibilité de rejeter tous les cookies « par un single clic ou tout moyen équivalent » du fait qu'elle aboutirait à une baisse drastique du taux de consentement des utilisateurs et risque de remettre en cause la pertinence d'une exemption à destination des médias. Elles souhaitent diminuer à 3 mois le délai durant**

Commission proposal	Drafting suggestions and Comments
	lequel il est interdit de solliciter de nouveau le consentement de l'utilisateur, afin de s'adapter au marché publicitaire valorisant des informations récentes sur les internautes. **Elles soulignent que toutes ces modifications supposent de vérifier au préalable l'existence de logiciels permettant de distinguer les différents consentements donnés pour un même site.**
Member States shall designate the competent supervisory authority under Regulation (EU) 2016/679 for the supervision and enforcement of the rules under this paragraph.	FR (Comments): **Les autorités françaises soutiennent les ajouts proposés par la Présidence pour introduire l'obligation pour les Etats membres de tous désigner leur autorité de protection des données pour appliquer la réglementation en matière de cookies. En effet, sans aller jusqu'à appliquer le mécanisme du guichet unique du RGPD qui ne serait pas nécessairement adapté dans ce contexte, s'assurer que ce seront les mêmes autorités qui appliqueront ces règles aura nécessairement pour effet d'accroître l'homogénéisation et la cohérence des pratiques en la matière. Ce choix est cohérent avec d'autres réglementations qui imposent la désignation des autorités de protection des données sans imposer le mécanisme du guichet unique (règlement IA, règlement publicité politique).** DK (Comments): We are concerned about the implications of having the competent supervisory authorities under the GDPR enforcing this Article and whether all the necessary changes have been made to the legal text. Specifically, we are concerned that Article 5(3) will be subject to the regulatory regime of the ePrivacy Directive, for instance with regards to sanctions, while the rules on consent (and perhaps also on the centralised consent mechanism) will be subject to other rules under the GDPR, and that the supervisory authorities will have to enforce rules on interrelated articles and for instance administer fines subject to two different regulatory regimes. It would be quite complex

Commission proposal	Drafting suggestions and Comments
	to navigate for both supervisory authorities and providers subject to the regulations. This could be a focus point during trilogue negotiations. FI (Comments): FI can support this proposal. SK (Comments): **SK question:** does this provision mean that only DPA will have the power to supervise both personal data and non-personal data? Will the national regulatory authorities referred to in Directive 2002/58/EC therefore have no power under this provision? Currently, only the NRA is competent in Slovakia under this provision (for both personal and non-personal data) and we need to know whether this will result in a change in the competent authority.
2a In Article 17, the following paragraph is added:	
3. Member States shall adopt and publish, by [24 months after the adoption of this Regulation] the laws, regulations and administrative provisions necessary to comply with Article 5(3). They shall immediately communicate the text of those measures to the Commission. **They should apply those measures from [24 months after the adoption of this Regulation].'**	MT (Comments): We support the longer transposition period of 24 months. SI (Comments): Republic of Slovenia welcomes the prolongation of the period for transposition into national law from 18 to 24 months. Nevertheless, we stand by our position that since the provisions of both the Digital Networks Act and the ePrivacy Directive are regulated in the same national legislation in most Member States, the deadlines for transposing the provisions related to the ePrivacy Directive in the Digital Omnibus and those in the Digital Networks Act should be harmonised.

Commission proposal	Drafting suggestions and Comments
Article 6 **Amendments to Directive (EU) 2022/2555**	CZ (Comments): CZ Red line: According to CZ, the text is moving in the right direction, but in some areas—particularly cross-border notification (Art. 23d)—it remains unclear how it should work in practice, including the role of ENISA and how data flows will be set up. CZ therefore proposes that these issues be clarified as set out below. .
Directive (EU) 2022/2555 is amended as follows:	
1. The following Article 23a is added:	
'Article 23a	DK (Comments): DK: The added value of now re-named "incident reporting information point" at EU level remains unclear to us, as ENISA could already create it.
~~Single entry point for~~ Incident reporting **information point**	
(1) ENISA shall develop and maintain ~~a single entry~~ **an incident reporting information** point to support the obligation to report incidents and related events under the Union legal acts where those Union legal acts provide so ('~~single entry~~ **incident reporting information** point'). ~~Without prejudice to Article 16 of Regulation (EU) 2024/2847 of the European Parliament and of the Council, ENISA may ensure that the single entry point builds on the single reporting platform established under that Regulation.~~	EE (Comments): Do we understand correctly that the single-information point is basically a website managed by ENISA? AT (Comments): Developing an incident reporting information point is significantly less complex than establishing a single-entry point. Thus, the resources necessary for the development differ considerably. This fact has to be kept in mind when simultaneously negotiating the CSA 2 in the HWP CI. The financial

Commission proposal	Drafting suggestions and Comments
	statement regarding the ENISA mandate has to be adapted and the current budgetary implications must be reflected accordingly.
~~(2) ENISA shall take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single-entry point and the information submitted or disseminated via the single-entry point. ENISA shall take into account the sensitivity of information submitted or disseminated pursuant to the Union legal acts referred to in paragraph (1) and ensure that competent authorities under those Union legal acts have access to and process the information as required under those Union legal acts.~~	
2a. The incident reporting information point shall:	
(a) enable the identification of applicable obligations to report incidents and related events referred to in paragraph 1;	BE (Drafting suggestions): **~~(a) enable the identification of applicable obligations to report incidents and related events referred to in paragraph 1;~~** BE (Comments): It is unclear what the difference is between paragraphs a and b, it seems paragraph b is sufficient. So suggestion to delete paragraph a.
(b) be designed to allow, on the basis of relevant information provided, to identify the applicable reporting obligations and to be redirected to the appropriate national entry point referred in Article 23b;	AT (Drafting suggestions): be designed to allow, on the basis of relevant information provided, to identify the applicable reporting obligations and to be redirected to the appropriate national ~~entry point referred in Article 23b;~~ **authorites and procedures;** AT (Comments):

Commission proposal	Drafting suggestions and Comments
	There should not be a reference to the NEP in Article 23b. The timelines of implementation differ and the reference therefore risks pointing to a non-existent structure. HU (Drafting suggestions): **(b) be designed to allow~~, on the basis of relevant information provided,~~ to identify the applicable reporting obligations and to be ~~redirected~~ *directed* to the appropriate national entry point referred in Article 23b;** HU (Comments): HU: As according to paragraph (2c) SIP would be designed that it shall not enable the submission, transmission, storage or processing of any incident notification or related data, and shall not collect any information allowing the identification of the notifying entity or of any incident, no information should be required to be provided by the entities or authorities. CZ (Drafting suggestions): **(b) be designed to allow, on the basis of relevant information provided, ~~to identify~~ the identification of the applicable reporting obligations and ~~to be the~~ redirect~~ed~~ion to the appropriate national entry point referred in Article 23b;** BE (Comments): Belgium welcomes the simplified text related to the incident reporting information point.

Commission proposal	Drafting suggestions and Comments
(c) make available simplified and documented information on incident notification processes in the different Member States, such as help guides or tutorials.	EE (Comments): Words "guides or tutorials" - should these guides also entail information on what to do if national entry point is not (yet) functioning? See also comment on recital 59 (alternative means for reporting incidents). HU (Drafting suggestions): **(c) make available simplified and documented information on incident notification processes in the different Member States~~, such as help guides or tutorials~~.** HU (Comments): HU: We propose the deletion of examples, as the expectation of developing a training material, a tutorial may also impose additional costs on Member States.
2b. When developing the incident reporting information point, ENISA shall consult the relevant national competent authorities under the relevant Union legal acts, the NIS Cooperation Group and the CSIRT Network. ENISA shall establish structured communication channels ensuring that information available on the single-information point is swiftly and effectively updated. Member States shall communicate to ENISA all relevant and necessary information for the purpose of paragraph 2a.	EE (Comments): First sentence - why only NIS CG and CSIRT Network? Should it also entail other similar groups from other EU Acts – such as: European Data Protection Board (see GDPR Article 68), Oversight Forum (see DORA Regulation Article 32), European Digital Identity Cooperation Group (see eIDAS Regulation Article 46e) and Critical Entities Resilience Group (see CER Directive Article 19)? And in the future, other relevant cooperation groups that are established under current or new EU Acts that might also have in the future the requirement to use national entry points (NEP) - what about those groups? Or should this reference be broader and more future proof?

Commission proposal	Drafting suggestions and Comments
	CZ (Drafting suggestions): **2b. ~~When developing the incident reporting information point, ENISA shall consult the relevant national competent authorities under the relevant Union legal acts, the NIS Cooperation Group and the CSIRT Network.~~ ENISA shall establish structured communication channels to ensur~~eing~~ that information available on the incident reporting ~~single~~ information point is swiftly and effectively updated. Member States shall communicate to ENISA all relevant and necessary information for the purpose of paragraph 2a.**
2c. The incident reporting information point shall not enable the submission, transmission, storage or processing of any incident notification or related data, and shall not collect any information allowing the identification of the notifying entity or of any incident.	CZ (Comments): CZ: CZ suggests simplifying this provision. Once the incident reporting information point is defined as an informational and navigational tool, it is already sufficiently clear that it is not intended to function as a reporting platform. The current wording is unnecessarily detailed and risks over-regulating a purely informational instrument. BE (Comments): Belgium supports this addition.
2d. After establishing the incident reporting information point and in cooperation with the NIS Cooperation Group, ENISA shall explore the possibility to extend the incident reporting information point by providing a report on:	EE (Comments): See previous comment on NIS2 Article 23a (2b). CZ (Drafting suggestions): **~~2d. After establishing the incident reporting information point and in cooperation with the NIS Cooperation Group, ENISA shall explore the~~**

Commission proposal	Drafting suggestions and Comments
	~~possibility to extend the incident reporting information point by providing a report on:~~ CZ (Comments): CZ: Since IRIP should serve as an information webpage, we believe that it is not necessary to include this part in such retails to the body of the directive or add new obligations to respective networks without clear added value. We propose to reflect the possibility to include this type of information to recitals; please see recital 49a.
(a) regulatory mapping of relevant EU legal acts imposing cybersecurity risk management measures;	EE (Comments): What is the added value on researching on other relevant EU legal acts imposing cybersecurity risk management obligations? CZ (Drafting suggestions): ~~(a) regulatory mapping of relevant EU legal acts imposing cybersecurity risk management measures;~~
(b) national measures, including transposition measures, implementing relevant Union legal acts imposing cybersecurity risk management obligations;	EE (Comments): What is the added value on researching on other relevant EU legal acts imposing cybersecurity risk management obligations? CZ (Drafting suggestions): ~~(b) national measures, including transposition measures, implementing relevant Union legal acts imposing cybersecurity risk management obligations;~~

Commission proposal	Drafting suggestions and Comments
(c) content to support entities in complying with obligations, in particular regarding entity registration, and cybersecurity risk-management.	EE (Comments): What is the added value on researching on entity registration and cybersecurity risk management obligations? CZ (Drafting suggestions): ~~**(c) content to support entities in complying with obligations, in particular regarding entity registration, and cybersecurity risk-management.**~~
~~(3) ENISA shall provide and implement the specifications on the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the single-entry point. ENISA shall develop the specifications in cooperation with the Commission, the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph (1). The specifications shall ensure that:~~	
~~(a) the necessary capability for interoperability with regard to other relevant reporting obligations referred to in paragraph (1) is ensured;~~	
~~(b) technical arrangements for the relevant entities and authorities under the Union legal acts referred to in paragraph (1) to access, submit , retrieve, transmit or otherwise process information from the single-entry point, are in place and, provide technical protocols and tools that allow the entities and authorities to further process the receive information within their systems;~~	
~~(c) the specificities of the incident reporting requirements set out under the Union legal acts referred to in paragraph (1) are duly taken into account;~~	

Commission proposal	Drafting suggestions and Comments
~~(d) where relevant, the single-entry point is interoperable and compatible with European Business Wallets referred to in [Proposal for a Regulation: Insert title of the proposal] and that the European Business Wallets can be used at least to identify and authenticate entities using the single-entry point;~~	
~~(e) entities using the single-entry point can retrieve and supplement information that they have previously submitted via the single-entry point;~~	
~~(f) a single notification of information submitted by an entity via the single-entry point can be used to fulfil reporting obligations as set out under any of the other Union legal acts which provide for incident reporting to the single-entry point.~~	
~~(4) Unless provided for in the Union legal acts referred to in paragraph (1) of this, ENISA shall not have access to the notifications submitted through the single-entry point.~~	
~~(5) Within [18] months from the entry into force of this Regulation, ENISA shall pilot the functioning of the single-entry point for each added Union legal act, including testing that takes into account the specificities and requirements for the notifications set out by each respective Union legal act, and after consulting the Commission and the relevant competent authorities under the respective Union legal acts. ENISA shall enable the notification of incidents under each Union legal act referred to in paragraph (1) only after piloting the functioning and after the Commission published a notice pursuant to paragraph 6.~~	
~~(6) The Commission shall, in cooperation with ENISA, assess the proper functioning, reliability, integrity and confidentiality of the single-entry point. When the Commission, after consultation of the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph 1, finds that the single-entry point ensures the proper functioning, reliability,~~	

Commission proposal	Drafting suggestions and Comments
~~integrity and confidentiality, it shall publish a notice to that effect in the Official Journal of the European Union.~~	
2. The following Article 23b is added:	LV (Drafting suggestions): (5) In the event which prevents the submission of single notification through the national entry point, Member States shall ensure that alternative channels are available for reporting of incidents and related events. LV (Comments): We would suggest to include as paragraph 5 the requirement for Member States to have alternative notification channels available in case the NEP is not available for subjects (corresponding to recital (57)).
'Article 23b	FR (Comments): The submission on this Article has been jointly developed with Italy and the Netherlands as a common approach.
National entry point for incident reporting	HU (Comments): HU still has concerns on the mandatory introduction of the national entry point. Therefore, our scrutiny reservation remains in place until a political decision is taken on the proposal.
(1) Member States shall establish and maintain a national entry point for the reporting of incidents and related events under the Union legal acts where those Union legal acts provide so. The national entry point shall enable entities to fulfil their notification obligations through a single notification at national level which reaches all relevant competent authorities.	NL (Drafting suggestions): **(1) Member States shall establish and maintain a national entry point for the reporting of incidents and related events under the Union legal acts where those Union legal acts provide so. The national entry point ~~shall enable entities to fulfil their notification obligations~~**

Commission proposal	Drafting suggestions and Comments
	~~through a single notification at national level which reaches all relevant competent authorities.~~ may carry out one or more tasks depending on national organisational arrangements, particularly: **(a) enabling the submission of notifications at national level;** **(b) receiving and process notifications submitted by entities;** **(c) ensuring or facilitate access to such notifications for the relevant competent authorities;** **(d) transmitting or make available relevant information to other national authorities, where necessary;** **(e) supporting coordination among competent authorities in relation to reported incidents or information;** **(f) providing guidance or assistance to entities regarding notification procedures;** **(g) performing any other function necessary to facilitate the effective management and sharing of notifications at national level.** NL (Comments): The submission has been jointly developed with ITA and FRA as a common approach. IT (Drafting suggestions): **(1) Member States shall establish and maintain a national entry point for the reporting of incidents and related events under the Union legal acts where those Union legal acts provide so. The national entry point ~~shall enable entities to fulfil their notification obligations through a single notification at national level which reaches all relevant competent authorities.~~ may carry out one or more tasks depending on national organisational arrangements, particularly:** **(a) enabling the submission of notifications at national level;**

Commission proposal	Drafting suggestions and Comments
	(b) receiving and process notifications submitted by entities; **(c) ensuring or facilitate access to such notifications for the relevant competent authorities;** **(d) transmitting or make available relevant information to other national authorities, where necessary;** **(e) supporting coordination among competent authorities in relation to reported incidents or information;** **(f) providing guidance or assistance to entities regarding notification procedures;** **(g) performing any other function necessary to facilitate the effective management and sharing of notifications at national level.** IT (Comments): We consider it essential to ensure that national entry points can serve a range of functions, taking into account national arrangements, the level of maturity of each Member State, and the specific characteristics of the national community. In this context, it is important to preserve sufficient flexibility for Member States, so that entry points can effectively act, where appropriate, as information hubs. FR (Drafting suggestions): **(1) Member States shall establish and maintain a national entry point for the reporting of incidents and related events under the Union legal acts where those Union legal acts provide so. The national entry point ~~shall enable entities to fulfil their notification obligations through a single notification at national level which reaches all relevant competent authorities~~ may carry out one or more tasks depending on national organisational arrangements, particularly:**

Commission proposal	Drafting suggestions and Comments
	(a) enabling the submission of notifications at national level; **(b) receiving and process notifications submitted by entities;** **(c) ensuring or facilitate access to such notifications for the relevant competent authorities;** **(d) transmitting or make available relevant information to other national authorities, where necessary;** **(e) supporting coordination among competent authorities in relation to reported incidents or information;** **(f) providing guidance or assistance to entities regarding notification procedures;** **(g) performing any other function necessary to facilitate the effective management and sharing of notifications at national level.** FR (Comments): While we recognise the need for nationla entry point to better support the notifying entities in their notification process, we consider the necessity for Member States to adapt this national entry point to their national reporting structures and their specificities (e. g. CER notifications on a classified information system in France). We believe therefore that our proposal enables more flexibility for Member States to implement their national entry point, in accordance with their national arrangements, while delineating the scope clearly. This broaden definition should enable a better adaption to the respective national specificities. EE (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	(1) Member States shall establish and maintain a national entry point for the reporting of incidents and related events under the Union legal acts where those Union legal acts provide so. The national entry point shall enable entities to fulfil their notification obligations through a single notification at national level which reaches all relevant <u>national</u> competent authorities <u>under the relevant Union legal acts</u>. AT (Comments): AT remains very critical regarding the mandatory establishment of national single-entry points. In ATs view the provision should be changed to a recommendation supporting the voluntary establishment of NEPs. In ATs opinion NEPs do not provide a clear added value. Neither for entities nor for the MS and its competent authorities. It is highly doubtful whether the mandatory establishment of purely national technical solutions is covered by the legal basis in Art 114 TFEU at all. AT therefore requests a legal review by the CLS. AT is sceptical if the establishment of purely national solutions is fit to promote the internal market, rather than promote further fragmentation. AT already has established reporting structures for every Union legal act in question. The systems are maintained independently by the competent authorities nationally designated according to every legal act. These authorities operate their systems independently. There is no shared technical solution across the systems. If a national entry point were to be established, the current reporting systems would need a comprehensive and cost-intensive technical revision and restructuring. Further, the establishment of NEPs requires close and intensive cooperation between the relevant authorities at national level, making the revision process even more complex. In times of serious budgetary constraints, a project of this financial magnitude does not seem feasible.

Commission proposal	Drafting suggestions and Comments
	In that context AT suggests (provided the proposal of NEPs is maintained) including the provision of financial means through the appropriate EU-funding mechanisms like the DEP. A reference shall also be added to the legal text to ensure the mandatory nature of financing at MS level through EU-funds. Furthermore, national centralisation does little to simplify cross-border reporting. Considering the above, AT maintains the position that mandatory establishing national single-entry points would lead to a disproportionate administrative burden and considerable overhead borne by the national authorities. CZ (Comments): CZ: CZ appreciates that the proposal offers flexibility enabling Member States to continue using their existing national solutions, including DORA frameworks. In this context, it is important to preserve room for national approaches and avoid creating unnecessary pressure to adapt systems and reporting mechanisms in which Member States have already invested substantially and which are functioning effectively. For CZ it is important that the proposal leaves the decision on the NEP design to the Member States, allowing them to choose the most suitable approach reflecting country specific conditions building on the interconnection of the already existing systems. PL (Comments): This is a crucial provision to ensure simplification goals. There should be one single entry at the national level, just like the compromise text states. It should remain unchanged. ES

Commission proposal	Drafting suggestions and Comments
	(Comments): Spain understands the expression "single notification at national level" in Article 23b(1) as referring to the simplification benefit for reporting entities, namely that an entity discharges its notification obligations across multiple regulatory frameworks through a single submission. This expression should not be read as requiring Member States to centralise all incident notifications, incident-related data or supervisory responsibilities in a single authority, system or repository. This reading is consistent with Article 23b(2), which expressly preserves Member States' flexibility to configure their national entry point in accordance with existing competent authority structures and the allocation of competences among authorities, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information. It is also consistent with recital 50a, which recognises that a national entry point may take the form of a digital interface, platform or technical interoperability hub. Spain considers that architectures in which the national entry point operates as a routing or interoperability mechanism (without a centralised data repository) are fully compatible with the text as drafted
(2) Member States shall retain flexibility to configure their national entry point in accordance with their existing competent authority structures and the allocation of competences among authorities, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information.	NL (Drafting suggestions): **(2) Member States shall retain flexibility to configure their national entry point in accordance with their existing ~~competent authority~~ national structures and the allocation of competences among authorities, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information.** NL (Comments): It is not only the competent authorities, and also inconsistent when looking at recital 50.

Commission proposal	Drafting suggestions and Comments
	IT (Drafting suggestions): **(2) Member States shall retain flexibility to configure their national entry point in accordance with their existing ~~competent authority~~ national structures and the allocation of competences among authorities, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information.** FR (Drafting suggestions): **(2) Member States shall retain flexibility to configure their national entry point in accordance with their existing ~~competent authority~~ national structures and the allocation of competences among authorities, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information.** FR (Comments): This modification enables consistency with recital 50. EE (Comments): Words “existing competent authority structure” - what "competent authority" is meant here? NIS2 Article's 8 competent authority? Or said NIS2 competent authorities + other competent authorities that are mentioned in other relevant Union legal acts? BE (Comments): Belgium strongly supports the addition of this paragraph.

Commission proposal	Drafting suggestions and Comments
	ES (Comments): See comment on Article 23b(1)
(3) Member States shall design their national entry point with a view to make the national entry points interoperable with the national entry points of the other Member States.	NL (Drafting suggestions): **(3) Member States ~~shall~~ may design their national entry point with a view to make the national entry points interoperable with the national entry points of the other Member States.** IT (Drafting suggestions): **(3) Member States ~~shall~~ may design their national entry point with a view to make the national entry points interoperable with the national entry points of the other Member States.** FR (Drafting suggestions): **(3) Member States ~~shall~~ may design their national entry point with a view to make the national entry points interoperable with the national entry points of the other Member States.** FR (Comments): While we fully recognise the need for interoperability, we consider it equally important that Member States retain an appropriate degree of control over their national entry points, including with regard to the implementation of necessary security features. CZ (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	(3) Member States shall design their national entry point with a view to making the national entry points interoperable with the national entry points of ~~the~~ other Member States. BE (Drafting suggestions): **(3) Member States shall design their national entry point with a view to make it ~~the national entry points~~ interoperable with the national entry points of the other Member States.** BE (Comments): Suggestion to remove one mention of "national entry points" and replace with "it". This is to make the text flow better.
(4) ENISA shall, by [12 months from the date of entry into force of this amending Regulation], in consultation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, provide guidelines to support Member States in the establishment, maintenance and secure operation of their respective national entry point. Those guidelines shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures. Those guidelines shall include the technical specifications necessary to ensure interoperability between all Member States' national entry points as referred to in paragraph 3 and to facilitate the alignment of incident notifications submitted via their respective national entry point with cross-border reporting obligations.	NL (Drafting suggestions): **(4) ENISA shall, by [12 months from the date of entry into force of this amending Regulation], in consultation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, provide ~~guidelines~~ non-binding recommendations to support Member States in the establishment, maintenance and secure operation of their respective national entry point. Those ~~guidelines~~ recommendations shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures. Those ~~guidelines~~ recommendations shall include the technical specifications necessary to ensure interoperability between all Member States' national entry points as referred to in paragraph 3 and to facilitate the alignment of incident notifications submitted via their respective national entry point with cross-border reporting obligations.** IT

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): **(4) ENISA shall, by [12 months from the date of entry into force of this amending Regulation], in consultation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, provide ~~guidelines~~ non-binding recommendations to support Member States in the establishment, maintenance and secure operation of their respective national entry point. Those ~~guidelines~~ recommendations shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures. Those ~~guidelines~~ recommendations shall include the technical specifications necessary to ensure interoperability between all Member States' national entry points as referred to in paragraph 3 and to facilitate the alignment of incident notifications submitted via their respective national entry point with cross-border reporting obligations.** IT (Comments): While we fully recognise the importance of ensuring interoperability, we consider it equally important that Member States retain an appropriate degree of control over their national entry points, including with regard to the implementation of necessary security features. FR (Drafting suggestions): **(4) ENISA shall, by [12 months from the date of entry into force of this amending Regulation], in consultation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, provide ~~guidelines~~ non-binding recommendations to support Member States in the establishment, maintenance and secure operation of their respective national entry point. Those ~~guidelines~~**

Commission proposal	Drafting suggestions and Comments
	recommendations shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures. Those ~~guidelines~~ recommendations shall include the technical specifications necessary to ensure interoperability between all Member States' national entry points as referred to in paragraph 3 and to facilitate the alignment of incident notifications submitted via their respective national entry point with cross-border reporting obligations. FR (Comments): In line with the comment on paragraph 4, while we recognise the need for recommendations from ENISA to support Member States in establishing their national entry point, we believe Member States should retain an appropriate degree of control over their national entry points, including with regard to the implementation of necessary security features. EE (Comments): First sentence - Why only NIS CG and CSIRT Network? See previous comment on NIS2 Article 23a (2b). LV (Drafting suggestions): **(4) ENISA shall, by [~~12 months from the date of~~ entry into force of this amending Regulation], in consultation with the CSIRTs network, the NIS Cooperation Group and competent authorities under the relevant Union legal acts, provide guidelines to support Member States in the establishment, maintenance and secure operation of their respective national entry point. Those guidelines shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures.**

Commission proposal	Drafting suggestions and Comments
	Those guidelines shall include the technical specifications necessary to ensure interoperability between all Member States' national entry points as referred to in paragraph 3 and to facilitate the alignment of incident notifications submitted via their respective national entry point with cross-border reporting obligations. LV (Comments): Guidelines by ENISA on technical, operational and organisational measures (Article 23b(4)) for national entry points and on harmonization of incident notifications (Article 23c(3)) should be developed before Regulation enters into force OR the 30 months deadline for the obligation to report via the national entry point should only start after work on these guidelines is concluded. If the development or adaptation of national entry points and work on these guidelines would occur in parallel, that would only create uncertainty for Member States and would hamper the overall process, including meeting the deadline. HU (Drafting suggestions): ~~**(4) ENISA shall, by [12 months from the date of entry into force of this amending Regulation], in consultation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, provide guidelines to support Member States in the establishment, maintenance and secure operation of their respective national entry point. Those guidelines shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures. Those guidelines shall include the technical specifications necessary to ensure interoperability between all Member States' national entry points as referred to in paragraph 3 and to facilitate the alignment of incident**~~

Commission proposal	Drafting suggestions and Comments
	~~**notifications submitted via their respective national entry point with cross-border reporting obligations.**~~ HU (Comments): HU: We have strong concerns on the schedule of tasks related to the harmonisation of law and NEP establishment. We are of the point that it would be more time- and cost-effective if based the report of the Commission and the guidelines of ENISA, the relevant union laws should be revised, and the development of NEPs would be expected after the harmonisation work is done. Thus, this paragraph should be incorporated to Art. 23c (3). *HU: As national entry points may become concentration points for highly sensitive incident-related information, including vulnerability data, trade secrets, information concerning critical infrastructure and operational data handled by competent authorities, we consider that the secure operation of the national entry point under this Article should be supported by minimum technical and organisational security controls. These should include strong authentication, segregation of access between competent authorities, encryption in transit and at rest, audit logging, regular review of access rights, retention limits, as well as availability and overload protection requirements. Since the national entry point may itself become a critical dependency during large-scale incident waves, alternative reporting channels should be tested in advance and properly documented. This point is also reflected in our comment on Recital 50.* CZ (Drafting suggestions): **(4) ENISA shall, by [12 months from the date of entry into force of this amending Regulation], in consultation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts including European advisory authorities and national**

Commission proposal	Drafting suggestions and Comments
	supervisory authorities in the financial market, provide non-binding guidelines to support Member States in the establishment, maintenance and secure operation of their respective national entry point. Those guidelines shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures. Those guidelines shall include ~~the~~ technical specifications ~~necessary~~ to ensure interoperability between all Member States' national entry points as referred to in paragraph 3 and to facilitate the alignment of incident notifications submitted via their respective national entry point with cross-border reporting obligations. CZ (Comments): CZ: In order to ensure legal certainty and clarity of the legislative text, CZ proposes to include explicitly the national financial supervisory authorities and the European Supervisory Authorities (ESAs) in Article 23b(4), 23(c) and 23d(2), as the proposal also covers financial institutions and the DORA framework BE (Comments): Belgium strongly supports the broadening of the consultation scope when it comes to the drafting of guidelines on the establishment, maintenance and operation of the National Entry Points. The National Entry Points are not only meant for NIS2 incident notifications, so it is crucial that other relevant authorities under the different acts are also included in this process. SE (Drafting suggestions): ENISA shall, by [12 months from the date of entry into force of this amending Regulation], in consultation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal

Commission proposal	Drafting suggestions and Comments
	acts, provide guidelines to support Member States in the establishment, maintenance and secure operation of their respective national entry point. Those guidelines shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures. These guidelines shall also ~~include the technical specifications necessary to ensure~~measures aimed at increased interoperability between all Member States' national entry points as referred to in paragraph 3 and to facilitate the alignment of incident notifications submitted via their respective national entry point with cross-border reporting obligations. SE (Comments): SE is sceptical about the detailed technical specifications to be produced on NEPs as part of the guidance that ENISA is proposed to develop under Article 23b(4). Does this information not risk constituting a vulnerability if it ends up in the wrong hands? The protection of the NEPs becomes essential, as these will constitute a central function for incident reporting across the entire Union. ES (Comments): Spain considers that the ENISA guidelines referred to in Article 23b(4) should explicitly take into account that certain incident notification frameworks may require specific configurations of the national entry point due to confidentiality, security classification or sectoral supervision requirements. This is particularly relevant for critical entities within the meaning of Directive (EU) 2022/2557 and for incident information whose centralisation or dissemination may create security risks. The reference in Article 23b(4) to "experiences and lessons learned from existing reporting structures" provides an appropriate basis for ENISA to address these configurations. Spain raised this point orally at the AGS meeting of 27 May

Commission proposal	Drafting suggestions and Comments
	2026 and considers it important that it be reflected in the guidelines from the outset.
3. The following article 23c is added :	
'Article 23c	
Harmonising incident notification framework	AT (Comments): AT can only emphasise once again that harmonisation seen as a necessary prerequisite and first step towards simplification regarding incident reporting. Only once the incident notification/reporting obligations set out in the various legal acts have been harmonised (in terms of timelines/deadlines as well as information content/common data), will single-entry points – whether established at national or EU-level – actually be able to achieve any kind of simplification and provide added value. Without harmonisation of the reporting obligations across legal acts the NEPs simply cannot provide significant added-value that outweighs the considerable administrative overhead they would cause. The envisaged goal "*to fulfil their notification obligations through a single notification*" laid out in Art 23b (1) of this proposal can not be achieved without further harmonisation. The diverging timelines and information content in the different reporting obligations make the fulfilment of every reporting obligation through one single notification basically impossible in practice. HU (Comments): HU: We have strong concerns on the schedule of tasks related to the harmonisation of law and NEP establishment. We are of the point that it would be more time- and cost-effective if based the report of the Commission and the guidelines of ENISA, the relevant union laws should be revised, and

Commission proposal	Drafting suggestions and Comments
	the development of NEPs would be expected after the harmonisation work is done. BE (Comments): Belgium supports the approach to further identify ways to harmonise the incident notification framework. Here as wel, Belgium supports the broadening of the consultation scope to the competent authorities under the relevant Union legal acts.
(1) By [6 months after the entry into force of this Regulation] the Commission shall submit a report to the European Parliament and to the Council outlining common definitions, thresholds, deadlines, formats and procedures applying to Article 23 of Directive (EU) 2022/2555, Article 19a (1a), Article 24 (2a) and Article 45a (3a) of Regulation (EU) 910/2014, Article 33 (1) of Regulation (EU) 2016/679, Article 19 (1) and (2) of Regulation (EU) 2022/2554, and Article 15(1) of Directive (EU) 2022/2557.	HU (Comments): HU: We consider that the Commission report should address overlaps between the "significant incident" under NIS2 and the "high risk" threshold under Article 33 of the amended GDPR, for example in the case of ransomware incidents involving personal data. CZ (Drafting suggestions): **(1) By [6 months after the entry into force of this Regulation] the Commission shall submit a report to the European Parliament and to the Council outlining common elements and differences in definitions, thresholds, deadlines, formats and procedures applying to Article 23 of Directive (EU) 2022/2555, Article 19a (1a), Article 24 (2a) and Article 45a (3a) of Regulation (EU) 910/2014, Article 33 (1) of Regulation (EU) 2016/679, Article 19 (1) and (2) of Regulation (EU) 2022/2554, and Article 15(1) of Directive (EU) 2022/2557.** RO (Comments): Please consider the comments from point 49.

Commission proposal	Drafting suggestions and Comments
The report shall in particular consider concrete steps and a timeline for introducing the unified approach to incident reporting under the Union legal acts.	CZ (Drafting suggestions): **The report shall in particular identify areas where further harmonisation may be appropriate and assess the need for possible Union-level measures, including, where relevant, proposals for legislative or implementing action and an indicative timeline ~~consider concrete steps and a timeline for introducing the unified approach to incident reporting under the Union legal acts~~** SE (Drafting suggestions): The report shall in particular consider concrete steps and a timeline for ~~introducing the unified approach~~further harmonisation efforts ~~to~~on incident reporting under the Union legal acts. SE (Comments): SE wonders what the wording 'the unified approach' means in this provision? For SE, it is essential that there isn't any ambiguity introduced here. Especially regarding the fact that MS have and will continue to have, where necessary, for the purpose of safeguarding their national security, the full right to: • impose additional legal requirements regarding incident reporting, • flexibly gather further information in the event of an incident at national level.

Commission proposal	Drafting suggestions and Comments
(3) Building on the report referred in paragraph (1), ENISA shall, in consultation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, develop guidelines to foster the harmonization of incident notifications. These guidelines shall, in particular:	EE (Comments): First sentence - Why only NIS CG and CSIRT Network? See previous comment on NIS2 Article 23a (2b). HU (Drafting suggestions): **(3) Building on the report referred in paragraph (1), ENISA shall, in ~~consultation~~ *cooperation* with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, *establish a cross-sector working group to* develop guidelines to foster the harmonization of incident notifications. These guidelines shall, in particular:** HU (Comments): HU: We believe that this work should be done with the stronger involvement of MSs, consultation is not enough for this purpose. Thus, we propose that a cross-sector working group be established for the further harmonisation of reporting procedures and templates. This would guarantee a more efficient involvement of the authorities involved. CZ (Drafting suggestions): **(3) Building on the report referred to in paragraph (1), ENISA shall, in consultation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts including European supervisory authorities and national supervisory authorities in the financial market, issue guidelines to establish a coherent framework for reporting under relevant Union legal acts, including the use of common notification templates ~~develop guidelines to foster the~~**

Commission proposal	Drafting suggestions and Comments
	~~**harmonization of incident notifications**~~**. These guidelines shall, in particular:** CZ (Comments): CZ: This approach is more consistent with the logic already reflected in recital 106 of Directive (EU) 2022/2555 and with the current practice of the NIS Cooperation Group regarding common notification templates. In order to ensure legal certainty and clarity of the legislative text, CZ proposes to include explicitly the national financial supervisory authorities and the European Supervisory Authorities (ESAs) in Article 23b(4), 23(c) and 23d(2), as the proposal also covers financial institutions and the DORA framework.
(a) Identify ways to further harmonise templates for entities but also between CSIRTs across different sectors and legislative frameworks;	HU (Comments): HU: It of utmost importance that templates already used under different legislation, should not be duplicated during the transition. CZ (Drafting suggestions): **(a) identify common elements and differences in templates for entities and between CSIRTs across different sectors and legislative frameworks** ~~**Identify ways to further harmonise templates for entities but also between CSIRTs across different sectors and legislative frameworks**~~**;**
(b) Provide a thorough analysis on the different sectoral thresholds, and, where appropriate, provide suggestions with regards to possible harmonization to improve efficiency;	EE (Comments): What does this analysis entail?

Commission proposal	Drafting suggestions and Comments
	Does it also entail an incident classification taxonomy (basically the same that EE proposed with 15.05 comments - *see general comment on NIS2 Article 23*)? For background - we proposed following amendment to NIS2 Article 23 – a new paragraph 3a: *´3a. In order to contribute to the provision of comparable information about incidents, ENISA shall, in cooperation with CSIRTs network and other relevant authorities, adopt incident classification taxonomy. Said taxonomy is mandatory for CSIRTs.´* HU (Comments): HU: We consider that the ENISA guidelines should address overlaps between the "significant incident" under NIS2 and the "high risk" threshold under Article 33 of the amended GDPR, for example in the case of ransomware incidents involving personal data. CZ (Drafting suggestions): **(b)** **analyse differences in sectoral thresholds and their impact on incident reporting ~~Provide a thorough analysis on the different sectoral thresholds, and, where appropriate, provide suggestions with regards to possible harmonization to improve efficiency~~;**
(c) Review the stages of incident notifications under different Union legal acts and recommend measures to streamline the process for entities.	EE (Comments): Does this also cover the aspect of harmonizing incident notification deadlines across relevant EU Acts? DK (Comments):

Commission proposal	Drafting suggestions and Comments
	DK: We welcome the report on ways to consider concrete steps and a timeline for introducing the unified approach to incident reporting under the Union legal acts. However, we wish for clarification in the text as to who ENISA shall present the guidelines to. We suggest the Council, as member states will be implementing the guidelines, but the Commission could also be included here. HU (Drafting suggestions): **(c) Review the stages of incident notifications under different Union legal acts and recommend measures to streamline the process for entities.** ***(d) provide guidelines to support Member States in the establishment, maintenance and secure operation of their respective national entry point. Those guidelines shall*** ***(da) address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures,*** ***(db) include the technical specifications necessary to ensure interoperability between all Member States' national entry points and to facilitate the alignment of incident notifications submitted via their respective national entry point with cross-border reporting obligations.*** HU (Comments): HU: We have strong concerns on the schedule of tasks related to the harmonisation of law and NEP establishment. We are of the point that it would be more time- and cost-effective if based the report of the Commission and the guidelines of ENISA, the relevant union laws should be revised, and the development of NEPs would be expected after the harmonisation work is

Commission proposal	Drafting suggestions and Comments
	done. Thus, paragraph (4) of Art. 23c should be incorporated to this paragraph. CZ (Drafting suggestions): **c) rReview the stages of incident notifications under different Union legal acts ~~and recommend measures to streamline the process for entities~~.**
ENISA shall present a first draft of these guidelines [by - within 12 months after the entry into force of this Regulation], and a final version within 18 months, and shall update them regularly thereafter.	LV (Drafting suggestions): **ENISA shall present a first draft of these guidelines [by ~~- within 12 months after~~ the entry into force of this Regulation], and a final version within ~~18~~ 6 months, and shall update them regularly thereafter.** LV (Comments): Guidelines by ENISA on technical, operational and organisational measures (Article 23b(4)) for national entry points and on harmonization of incident notifications (Article 23c(3)) should be developed before Regulation enters into force OR the 30 months deadline for the obligation to report via the national entry point should only start after work on these guidelines is concluded. If the development or adaptation of national entry points and work on these guidelines would occur in parallel, that would only create uncertainty for Member States and would hamper the overall process, including meeting the deadline.
~~(7) Where the Commission finds in its assessment that the single-entry point does not ensure the proper functioning, reliability, integrity or confidentiality, ENISA shall take, in cooperation with the Commission and without undue delay, all necessary corrective measures to ensure the proper~~	

Commission proposal	Drafting suggestions and Comments
~~functioning, reliability, integrity or confidentiality without delay and inform the Commission of the results. Thereafter, the Commission shall reassess the proper functioning, reliability, integrity or confidentiality of the single-entry point and shall publish a notice in accordance with paragraph 6.~~	
4. The following article 23d is added:	
'Article 23d	
Cross-border incident notification	HU (Comments): HU: We propose to imply the definition of "relevant tools" to the directive as well.
(1) Member States should aim at facilitating cross-border notifications to multiple national reporting structures.	CZ (Drafting suggestions): **(1) Member States should aim at facilitating cross-border notifications between national entry points, where incidents have cross-border impacts ~~to multiple national reporting structures.~~** BE (Comments): While Belgium fully supports interoperability and the facilitation of cross-border notifications through common standards and harmonised reporting mechanisms, the current wording could be interpreted as suggesting that a single notification at group level (e.g. a financial group under the DORA regulation) may suffice for incidents affecting multiple entities across jurisdictions. In this regard, Belgium recalls that under DORA, incident reporting and impact assessments are conducted at the level of the individual legal financial entity, rather than at the level of a multinational financial group. Consequently, where an incident affects several legal entities established in

Commission proposal	Drafting suggestions and Comments
	different Member States, the relevant reporting obligations remain applicable to each affected entity and competent authority.
(2) ENISA shall, in consultation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, harmonise its relevant tools with national incident notification templates and facilitate an automatisation process to exchange information about cross-border impacts.	EE (Comments): Why only NIS CG and CSIRT Network? See previous comment on NIS2 Article 23a (2b). LV (Drafting suggestions): **(2) ENISA shall, in consultation with the CSIRTs network, the NIS Cooperation Group and competent authorities under the relevant Union legal acts, harmonise its relevant tools with national incident notification templates and ~~facilitate~~ support voluntary automation of information ~~an automatisation process to~~ exchange ~~information~~ about cross-border impacts.** LV (Comments): As there are no guidelines in place, it is unclear what kind of information would be shared through the automated process. Therefore, any automated processes at this point should be voluntary for Member States. HU (Drafting suggestions): **(2) ENISA shall, in ~~consultation~~ *cooperation* with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, harmonise its relevant tools with national incident notification templates and facilitate an automatisation process to exchange information about cross-border impacts.** HU (Comments):

Commission proposal	Drafting suggestions and Comments
	HU: We believe that this work should be done with the close involvement of MSs, consultation is not enough for this purpose. CZ (Drafting suggestions): **(2) ENISA shall, in consultation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts including European supervisory authorities and national supervisory authorities in the financial market, ~~harmonise its relevant tools with national incident notification templates and~~ facilitate an automatisation process to exchange information ~~about~~ between national entry points on cross-border impacts of incidents.** CZ (Comments): CZ: the wording *"harmonise its relevant tools with national incident notification templates"* appears redundant, as it is already covered by Article 23b. As mentioned above, in order to ensure legal certainty and clarity of the legislative text, CZ proposes to include explicitly the national financial supervisory authorities and the European Supervisory Authorities (ESAs) in Article 23b(4), 23(c) and 23d(2), as the proposal also covers financial institutions and the DORA framework. BE (Comments): What is meant here with "relevant tools" and "automatisation", especially in relation to notification templates and cross-border sharing of information? Does this mean de facto that the use of specific tools will be imposed on Member States to facilitate cross-border notifications?

Commission proposal	Drafting suggestions and Comments
	PL (Comments): We are aiming to have the same templates within EU27, hence the implementing acts. Why the provision refers to national incident notification templates? It seems it should refer to national platforms
(3) Information submitted through relevant tools shall not be automatically transmitted to ENISA in full, Member States shall have the possibility to select information shared.'	LV (Drafting suggestions): **(3) Information submitted through relevant tools shall not be automatically transmitted to other [possibly affected] Member States or ENISA in full, Member States shall have the possibility to select information shared.[2]** LV (Comments): It should be envisaged that Member State shall have possibility to select information shared not only with ENISA but also with other Member States as incidents may contain sensitive information and directly affect national security interests. CZ (Drafting suggestions): **(3) Information submitted through the automatisation process referred to in paragraph 2~~relevant tools~~ shall not be automatically transmitted to ENISA ~~in full~~, Member States shall retain control over the scope of information shared and any access to such information ~~have the possibility to select information shared~~.'** BE (Comments): Paragraph (3)still lacks clarity and would benefit from further specification.

Commission proposal	Drafting suggestions and Comments
	First, the reference to "information submitted through relevant tools" is ambiguous. It is unclear what category of information is covered. In particular, it should be clarified whether this refers to incident notification data, as such information will be submitted via national systems and tools. Second, the notion of "relevant tools" is not clear. Does it refer to national tools operated by Member States, or the use of specific tools at Union level. In the latter case, it should be clearly stated whether Member States would be required to adopt or use such tools for the purpose of sharing information with ENISA. The interaction between national reporting mechanisms and any potential Union-level tools should be further elaborated to avoid operational uncertainty.
2. Article 23 is amended as follows:	EE (Comments): - If the timeline harmonization is not done, then the proposed NEP shall help with doing the notification to relevant authorities, but it also means that the entity is expected to use the NEP several times for notifying one incident. - Since the Digital Omnibus's aim is to simplify doing the reporting of incidents, then it is essential that this matter is also solved and taken care of.
(a) in paragraph 1, the first sentence is replaced by the following:	
'Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of this Article of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 of this Article (significant incident) via the ~~single-entry~~**national entry** point ~~established~~ pursuant to Article ~~23a~~**23b**.	

Commission proposal	Drafting suggestions and Comments
The following paragraph 1b is added:	EE (Comments): This mentions "1b", but the next line says "b" - what is the correct new paragraph? Should the new paragraph be 1a not 1b – since currently there is no 1b?
(b) ENISA shall, in cooperation with the Cooperation Group, provide a mapping of all the competent authorities and CSIRTs referred to in paragraph 1 in the single information point established pursuant to Article 23a. '	EE (Drafting suggestions): **(1b) ENISA shall, in cooperation with the Cooperation Group, provide a mapping of all the competent authorities and CSIRTs referred to in paragraph 1 in the ~~single~~ incident reporting information point established pursuant to Article 23a. '** EE (Comments): See previous comment for the paragraph number. Words "single information point" - should this be "incident reporting information point"? LV (Drafting suggestions): **(b) ENISA shall, in cooperation with the NIS Cooperation Group, provide a mapping of all the competent authorities and CSIRTs referred to in paragraph 1 in the single information point established pursuant to Article 23a. '** CZ (Drafting suggestions): **(b) ENISA shall, in cooperation with the Cooperation Group, make available information on competent authorities and CSIRTs in the**

Commission proposal	Drafting suggestions and Comments
	incident reporting information point. ~~provide a mapping of all the competent authorities and CSIRTs referred to in paragraph 1 in the single information point established pursuant to Article 23a~~. ’
(b) the following paragraph 12 is added:	
‘When a manufacturer notifies a severe incident pursuant to Article 14(3) of Regulation (EU) 2024/2847 and the incident reporting under that Article contains relevant information as required under paragraph 4 of this Article, the reporting of the manufacturer under Article 14(3) of Regulation (EU) 2024/2847 shall constitute reporting of information under paragraph 4 of this Article.;’	
3. in Article 30, paragraph 1 is replaced by the following:	
‘1. Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis via ~~the single entry~~ **national entry** point ~~established pursuant to~~ **referred to in** Article ~~23a~~**23b**, by:	
(a) essential and important entities with regard to incidents, cyber threats and near misses;	
(b) entities other than those referred to in point (a), regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses.’	EE (Comments): Should this also contain “incidents”, not only “significant incidents”?
Article 7 **Amendment of Regulation (EU) 910/2014**	
Regulation (EU) 910/2014 is amended as follows:	

Commission proposal	Drafting suggestions and Comments
1. in Article 19a, the following paragraph 1a is inserted:	
'1a. Notifications pursuant to paragraph 1, point (b) of this Article to the supervisory body and, where applicable, to other relevant competent authorities, shall be made through the ~~single-entry~~ **national entry** point pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555.;'	
2. in Article 24, the following paragraph 2a is inserted:	
'2a. Notifications pursuant to in paragraph 2, point (fb), of this Article to the supervisory body and, where applicable, to other relevant competent bodies, shall be made through the ~~single-entry~~ **national entry** point pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555.;'	
3. in Article 45a the following paragraph 3a is inserted:	
'3a. Notifications pursuant to in paragraph 3 to the Commission and to the competent supervisory body, shall be made through the ~~single-entry~~ **national entry** point pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555.'	

Article 8 **Amendments to Regulation (EU) 2022/2554**	EE (Drafting suggestions): X. in Article 30, the following paragraph 4a is inserted: ´4a. Full contract may be prepared as part of a document provided by another legal instrument. ICT third-party service provider can prove compliance with requirements in paragraphs (1) and (2) with cybersecurity risk management measures that are documented due to requirements set in Article 21 of Directive (EU) 2022/2555 if said article applies to ICT third-party service provider.´ EE (Comments): EE proposes again an amendment to DORA Article 30 – a new paragraph 4a: *´4a. Full contract may be prepared as part of a document provided by another legal instrument. ICT third-party service provider can prove compliance with requirements in paragraphs (1) and (2) with cybersecurity risk management measures that are documented due to requirements set in Article 21 of Directive (EU) 2022/2555 if said article applies to ICT third-party service provider.´* Explanation: As a general rule, entities falling under the DORA are exempted from following NIS2, especially its risk management measures (Article 21 of NIS2). Then again, in practice there are ICT third-party service providers who also need to follow NIS2 requirements and DORA requirements. In DORA those entities are named as “ICT third-party service providers” and in NIS2 they are “managed service providers” and/or “managed security service providers”. When ICT third-party service providers provide services to financial entities (*see DORA Article 2 (1) (a)-(t)*), then those ICT third-party service providers are part of financial entity’s ecosystem and/or part of the services that the financial entity provides. Therefore, there is an assumption that ICT third-party service providers need to follow requirements of DORA

Commission proposal	Drafting suggestions and Comments
	– then again, they also need to follow NIS2. DORA article 28 (5) first sentence sets how the financial entity and ICT third-party service provider make the contractual agreement. Said agreement's content is regulated in DORA Article 30. At the same time, the same entity (*in terms of DORA "ICT third-party service provider" and in terms of NIS2 the "managed service provider" and "managed security service provider"*) needs to follow the cybersecurity risk management measures foreseen in Article 21 of NIS2, that are further specified in Commission Implementing Regulation (EU) 2024/2690. The same entities are also subject to supervision of the competent authorities of NIS2. In practice, DORA Article 30 has not made things easier for entities that need to follow NIS2 requirements. Said DORA Article has made it so that each financial entity requires from the ICT third-party service provider (that is also subject to NIS2) to duplicate and restructure their cybersecurity risk management measures that are in place, to the needs of each financial entity. This means that there is the need to duplicate the same work for different financial entities – and that work does not enhance the level of cybersecurity, but it raises the administrative burden and costs of the ICT third-party service provider(s). Currently, the interplay between NIS2 and DORA means that the same ICT service provider needs to do tailor-made documentations for each financial entity and/or for competent authorities in NIS2 and DORA.
Article 19 of Regulation (EU) 2022/2554 is amended as follows:	SE (Comments): SE would prefer it to be optional for Member States whether to perform incident reporting through the National Entry Point. Contrary to inducing simplification, mandatory reporting through NEP might impose a new administrative burden on both authorities and companies. The matter should therefore rather be discussed during the upcoming review of DORA (see article 58 in the DORA).
1. in paragraph 1, the first subparagraph is replaced by the following:	

Commission proposal	Drafting suggestions and Comments
'Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 via the ~~single-entry~~ **national entry** point established pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555 in accordance with paragraph 4 of this Article.'	AT (Comments): AT is of the opinion that under the **current** proposal, mandating a **national single-entry point**, Regulation (EU) 2022/2554 shall not be changed. Thus, DORA reporting should not become part of the consolidated incident reporting framework covered by a national single-entry point. RO (Comments): The compromise text is unclear, as it is not evident whether the intention is for the Regulation to be applied initially only to cybersecurity incidents covered by the NIS framework and subsequently extended, based on the report to be prepared by the Commission pursuant to Article 6(3), first subparagraph. In this context, further clarification is required, particularly in light of the timelines set out in Article 8. Please also consider the provisions of 50a, 50b, art. 6 point.1 – adding art. 23a para.(1) point. 2d)
2. in paragraph 2, the first subparagraph is replaced by the following:	
'Financial entities may, on a voluntary basis, notify via the ~~single-entry~~ **national entry** point established pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555 significant cyber threats to the relevant competent authority when they deem the threat to be of relevance to the financial system, service users or clients. The relevant competent authority may provide such information to other relevant authorities referred to in paragraph 6.'	AT (Comments): AT is of the opinion that under the **current** proposal, mandating a **national single-entry point**, Regulation (EU) 2022/2554 shall not be changed. Thus, DORA reporting should not become part of the consolidated incident reporting framework covered by a national single-entry point.
Article 9 **Amendments to Directive (EU) 2022/2557**	
Article 15 of Directive (EU) 2022/2557 is amended as follows:	
1. in paragraph 1, the first sentence is replaced as follows:	

Commission proposal	Drafting suggestions and Comments
'Member States shall ensure that critical entities notify via the ~~single-entry~~ **national entry** point established pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555 the competent authority, without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services.;'	LV (Comments): Scrutiny reservation with regard to Directive (EU) 2022/2557 (CER). The provisions of the Digital Omnibus affecting the CER Directive should first be assessed at expert level within the PROCIV-CER Working Party, where the CER framework was originally examined and negotiated. Expanded position: • LV has serious concerns regarding the inclusion of the CER Directive within the scope of the Digital Omnibus and cannot support such an approach. LV considers that the critical infrastructure resilience framework should be fully excluded from the envisaged horizontal incident reporting and administrative burden reduction mechanisms. • The CER Directive regulates matters directly linked to national security, the protection of critical infrastructure, civil protection and crisis management, as well as the handling of sensitive information. Integrating these matters into a single horizontal incident reporting system creates risks regarding the protection of critical infrastructure-related information, the separation of responsibilities between competent authorities, and the ability of Member States to apply processes aligned with their national security interests. We further recall that both the CER and NIS2 frameworks are "Directives", which provide Member States with a certain degree of discretion and flexibility in their national transposition and implementation. • Furthermore, the objectives and underlying logic of the CER Directive differ substantially from cyber security and digital incident reporting regimes. Within the CER framework, the assessment of incidents, risks and resilience measures is closely linked to sector-specific and national security considerations. Therefore, subjecting this framework to a single Digital Omnibus approach would not be proportionate.

Commission proposal	Drafting suggestions and Comments
	• It would neither be justified nor proportionate to require that non-cyber incidents — such as natural hazards, technical accidents, or physical/human-induced threats (including physical sabotage or terrorism) — be reported through the NIS2 contact point. • Physical incidents, which form the core of the CER Directive, should be reported exclusively to the national competent authorities designated under the CER framework, using the channels established by each Member State in the course of national transposition and implementation of the CER Directive. • The EU framework may promote mechanisms for the establishment of a national entry point with a view to reducing administrative burden; however, it should not impose a uniform organisational model. Member States must retain the necessary flexibility to organise reporting channels in accordance with their internal administrative structures and specific operational needs. • Consequently, LV does not consider it is appropriate for ENISA to develop a single notification template for incidents unrelated to cyber security or the digital environment (i.e. physical incidents). • The CER Directive has only recently been transposed, or is still in the process of transposition, in several Member States (approximately one third of Member States). Therefore, there is currently insufficient basis to conclude that horizontal amendments aimed at reducing administrative burden are necessary. Before any such amendments are pursued, a comprehensive assessment of the implementation and practical application of the CER framework across Member States would be required. Therefore, LV considers that the CER Directive should be excluded from the scope of the Digital Omnibus in order to preserve Member States' discretion in matters relating to the resilience and protection of critical infrastructure.

Commission proposal	Drafting suggestions and Comments
2. in paragraph 2, the following sub-paragraph is added:	
'The Commission may adopt implementing acts further specifying the type and format of information notified pursuant to Article 15(1). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 24(2).'	
Article 10 **Amendments, repeals and transitory clauses**	
1. Regulation 2019/1150/EU is ~~repealed with effect from [date = entry into application of this Regulation].~~ **amended as follows:**	AT (Comments): AT thanks the Presidency for the amendments made in the compromise text. AT welcome the changes made in the P2B-Regulation, whereby Article 4 and Article 11 are to remain in force indefinitely without a sunset clause. We therefore consider the text in its current form to strike a good balance, as provisions are repealed in the interests of simplification, whilst the relevant provisions for the protection of business users remain in place. In the long term, with a view to avoiding duplication, consideration could also be given to integrating the provisions for the protection of business users into the DSA. However - as the DSA is not currently under discussion - we consider this to be a good interim solution. However, for the sake of completeness, we would like to note the following: • Even if Article 14 (regarding "Judicial proceedings by representative organisations or associations and by public bodies") is deleted, from our understanding there is no need to amend the national enforcement systems (which in Austria are based on an effective system with cease

Commission proposal	Drafting suggestions and Comments
	and desist orders), as Article 15 remains unchanged and this leaves room for Member States to decide on their enforcement system. • Furthermore, we regret the deletion of Article 18, as an evaluation of the (remaining) provisions would appear beneficial.] FI (Comments): Although FI primarily supports the repeal of the P2B Regulation, FI can be flexible and support the Presidency compromise proposal concerning Article 10 and recital 59.
Articles 2(11), 2(12), 6, 8 to 10, 12 to 14, and 16 to 18, are deleted as of [date of entry into force].	NL (Drafting suggestions): **Articles 2(11), 2(12), 6, 8 to 10, 12 to 14, 16, 17 and 18 (2-4), are deleted as of [date of entry into force].** NL (Comments): Comments by NL: We greatly appreciate the efforts taken by the Presidency for responding to our joint call regarding maintaining several articles of the P2B regulation to provide the necessary protection for SMEs. We hereby thank the Presidency. Should the Presidency see room for one last small, technical adjustment, we would like to ask for the following: • In order to ensure the remaining articles of the P2B regulation are reviewed on a structural basis, it would be good to maintain Article 18 (1) P2B. This way, the P2B regulation will be reviewed every three years. IT (Comments):

Commission proposal	Drafting suggestions and Comments
	ITALY welcomes the new version of Recital 59 and Article 10 of the Digital Omnibus (P2B Regulation). In particular, Italy appreciates that the revised Presidency compromise proposal extends the scope of the provisions to be preserved by also including Articles 4 and 11, for which a transitional period had originally been envisaged. Italy supports the Presidency's approach aimed at preserving, for the purposes of legal certainty and maintaining the necessary level of protection for business users, selected definitions in Article 2, the provisions on terms and conditions in Article 3, on restrictions and suspensions in Article 4, on ranking in Article 5, on differentiated treatment in Article 7, on the internal complaint-handling system in Article 11, as well as the provisions in Article 15 ensuring enforcement. In Italy's view, maintaining these provisions in force contributes to safeguarding legal certainty, ensuring regulatory coherence across the Union acquis, and preventing gaps in the protection afforded to business users.
~~2. By way of derogation from paragraph 1, the following provisions shall continue to apply until 31 December 2032:~~	IT (Comments): ITALY welcomes the new version of Recital 59 and Article 10 of the Digital Omnibus (P2B Regulation). In particular, Italy appreciates that the revised Presidency compromise proposal extends the scope of the provisions to be preserved by also including Articles 4 and 11, for which a transitional period had originally been envisaged. Italy supports the Presidency's approach aimed at preserving, for the purposes of legal certainty and maintaining the necessary level of protection for business users, selected definitions in Article 2, the provisions on terms and conditions in Article 3, on restrictions and suspensions in Article 4, on ranking in Article 5, on differentiated treatment in Article 7, on the internal complaint-handling system in Article 11, as well as the provisions in Article 15 ensuring enforcement. In Italy's view, maintaining these provisions in force contributes to safeguarding legal certainty, ensuring regulatory

Commission proposal	Drafting suggestions and Comments
	coherence across the Union acquis, and preventing gaps in the protection afforded to business users
~~(a) Article 2, point (1);~~	
~~(b) Article 2, point (2);~~	
~~(c) Article 2, point (5);~~	
~~(d) Article 4;~~	
~~(e) Article 11;~~	
~~(f) Article 15.~~	
3. The following acts are repealed, with effect from [Date, aligned with the entry into application of the amendments]:	
a) Regulation (EU) 2022/868;	
b) Regulation (EU) 2018/1807;	
c) Directive 2019/1024.	
4. References to Regulation (EU) 2022/868, Regulation (EU) 2018/1807 and Directive 2019/1024 shall be read in accordance with the correlation table set out in Annex I of this Regulation.	
Article 11 **Final provisions**	
This Regulation shall enter into force on the third day following that of its publication in the Official Journal of the European Union.	

Commission proposal	Drafting suggestions and Comments
Articles under Chapter VIIc shall enter into application 18 months after the publication in the Official Journal of the European Union.	
~~Deviating from paragraph 3,~~ Article 5(2) shall enter into application 6 months after the publication in the Official Journal of the European Union.	LV (Drafting suggestions): "Article 5(2) shall enter into application ~~**6 months**~~ **24 months**...". LV (Comments): Member States need sufficient time to implement the provisions; therefore, the deadline for implementing the amendments to Directive 2002/58/EC should be 24 months. The deadline for transposing the Directive should also be considered the period during which service providers can prepare by developing solutions as provided for in Article 5(2) of the proposal regarding the amendments to Article 5(3) of Directive 2002/58/EC.
By way of derogation from paragraph 1, Article 3(8), points (a) to (c), Articles 6 (2) and (3) and 7 to 9, shall enter into application 18 months from the entry into force of this Regulation. ~~Deviating~~**By way of derogation** from the first sentence~~, where the Commission finds in its assessment pursuant to Article 23a (7) of Directive (EU) 2022/2555 that the single-entry point does not ensure the proper functioning, reliability, integrity or confidentiality~~, the obligations to report via the ~~single-entry~~**national entry** point set out in Article ~~23(4)~~**23b** of Directive (EU) 2022/2555, Article 19a (1a), Article 24 (2a) and Article 45a (3a) of Regulation (EU) 910/2014, Article 33 (1) of Regulation (EU) 2016/679, Article 19 (1) and (2) of Regulation (EU) 2022/2554, and Article 15(1) of Directive (EU) 2022/2557 shall enter into application ~~24~~**30** months from the entry into force of this Regulation.	IT (Drafting suggestions): **By way of derogation from paragraph 1,** Article 3(8), points (a) to (c), Articles 6 (2) and (3) and 7 to 9, shall enter into application 18 months from the entry into force of this Regulation. ~~Deviating~~**By way of derogation** from the first sentence~~, where the Commission finds in its assessment pursuant to Article 23a (7) of Directive (EU) 2022/2555 that the single-entry point does not ensure the proper functioning, reliability, integrity or confidentiality~~, the obligations to report via the ~~single-entry~~**national entry** point set out in Article ~~23(4)~~**23b** of Directive (EU) 2022/2555, Article 19a (1a), Article 24 (2a) and Article 45a (3a) of Regulation (EU) 910/2014, Article 33 (1) of Regulation (EU) 2016/679, Article 19 (1) and (2) of Regulation (EU) 2022/2554, and Article 15(1) of Directive (EU) 2022/2557 shall enter into application ~~24~~**30**~~30~~**36** months from the entry into force of this Regulation. FR

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): **By way of derogation from paragraph 1,** Article 3(8), points (a) to (c), Articles 6 (2) and (3) and 7 to 9, shall enter into application 18 months from the entry into force of this Regulation. ~~Deviating~~**By way of derogation** from the first sentence~~, where the Commission finds in its assessment pursuant to Article 23a (7) of Directive (EU) 2022/2555 that the single-entry point does not ensure the proper functioning, reliability, integrity or confidentiality~~, the obligations to report via the ~~single-entry~~**national entry** point set out in Article ~~23(4)~~**23b** of Directive (EU) 2022/2555, Article 19a (1a), Article 24 (2a) and Article 45a (3a) of Regulation (EU) 910/2014, Article 33 (1) of Regulation (EU) 2016/679, Article 19 (1) and (2) of Regulation (EU) 2022/2554, and Article 15(1) of Directive (EU) 2022/2557 shall enter into application ~~24~~~~30~~ **36** months from the entry into force of this Regulation. FR (Comments): This submission has been jointly developed with Italy and the Netherlands as a common approach. We believe that an extension of the deadline would enable Member States to better implement the national entry point. Indeed, its creation will require important coordination time with all the competent authorities at national level. Moreover, it will enable sufficient time for ENISA to provide it recommendations. LV (Comments): LV sees that it would be valuable to keep reference that deadline for the obligation to report via the national entry point could be extended by 6 months if deemed necessary to keep flexibility as not all Member States have established national entry points that not only will have to be developed but also tested.

Commission proposal	Drafting suggestions and Comments
	The guidelines by ENISA on technical, operational and organisational measures (Article 23b(4)) for national entry points and on harmonization of incident notifications (Article 23c(3)) should be developed before Regulation enters into force OR the 30 months deadline for the obligation to report via the national entry point should only start after work on these guidelines is concluded. If the development or adaptation of national entry points and work on these guidelines would occur in parallel, that would only create uncertainty for Member States and would hamper the overall process, including meeting the deadline. HU (Comments): HU: 12 months, after receiving the final guidelines prepared by ENISA, is longer that the previously proposed 6 months, but is still not enough for development of such a system, including the time required for elaboration of technical specifications with all organizations involved, conduct the public procurement, conclude a contract, develop, test and deploy the system.
This Regulation shall be binding in its entirety and directly applicable in all Member States.	
Done at Brussels,	
For the European Parliament *For the Council*	
The President *The President*	
	IT (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	IT drafting suggestions in red] *(112) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange, including annual and repetitive exchange, between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters [...]* Article 49 **Derogations for specific situations** 1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; (d) the transfer is necessary for important reasons of public interest;

Commission proposal	Drafting suggestions and Comments
	(e) the transfer is necessary for the establishment, exercise or defence of legal claims; (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case. Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued. The requirement that the transfer be non-repetitive shall not apply to transfers based on point (d) of the first subparagraph, where such transfers are necessary for important reasons of public interest recognised in Union law or in the law of a Member State, including transfers carried out pursuant to international or administrative agreements on mutual assistance or cooperation. 2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the

Commission proposal	Drafting suggestions and Comments
	register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients. 3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers. 4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject. 5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission. 6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30. IT (Comments): IT Comments: In general, we suggest amending recital 112 as well as article 49 of the GPDR within the framework of the omnibus package, as this is essential to resolving the existing uncertainty regarding the transfer of tax related data to third countries. A stable and adequate solution is needed, which requires a unified EU approach; otherwise, there is a real risk that exchanges of tax information with key jurisdictions lacking EU level data protection standards could collapse, seriously undermining efforts to fight international tax evasion. The revision of the recital is essential to include a clear and express derogation relating to the automatic exchange of information which is annual and repetitive.

Commission proposal	Drafting suggestions and Comments

Commission proposal	Drafting suggestions and Comments
	The proposed revision of article 49 expressly states that the exchange of information carried out on the basis of an international agreement on mutual assistance or cooperation falls under the public interest derogation even if the transfers are repetitive.